PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 9/32 — A1

(11) International Publication Number: **WO 00/48360**

(43) International Publication Date: 17 August 2000 (17.08.00)

(21) International Application Number: PCT/US00/03550

(22) International Filing Date: 11 February 2000 (11.02.00)

(30) Priority Data:

60/119,892	12 February 1999 (12.02.99)	US
60/119,958	12 February 1999 (12.02.99)	US

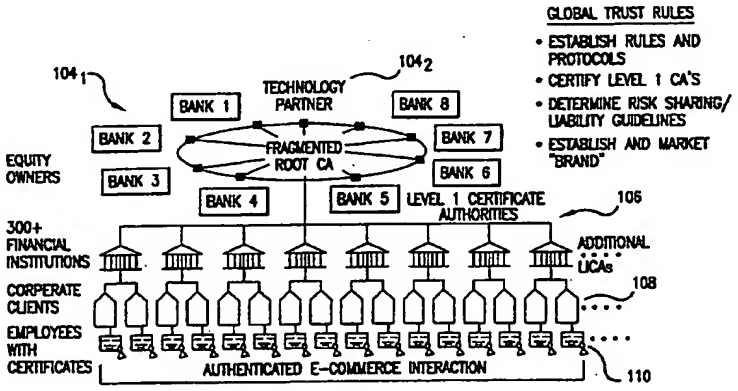
(71)(72) Applicants and Inventors: HICKS, Mack [US/US]; 4th floor, 201 3rd Street, San Francisco, CA 94103 (US). SEILER, Regina [US/US]; 4th floor, 201 3rd Street, San Francisco, CA 94103 (US). TALLENT, Guy, S., Jr. [US/US]; 16th floor, 140 East 45th Street, New York, NY 10017 (US). KUPRES, Kristin [US/US]; 16th floor, 140 East 45th Street, New York, NY 10017 (US). FREUDENSTEIN, Allen [US/US]; 55 Broad Street, New York, NY 10004 (US).

(74) Agents: RADDING, Rory, J., et al.; Pennie & Edmonds LLP, 1155 Avenue of the Americas, New York, NY 10036 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: SYSTEM AND METHOD FOR PROVIDING CERTIFICATION-RELATED AND OTHER SERVICES



(57) Abstract

A system for warranting the identity of a party over an electronic network is comprised of a root entity (102) and a plurality of additional entities (104, 106, 108 and 110). Each additional entity (104, 106, 108 and 110) is admitted to the system after agreeing to abide by a plurality of operating rules promulgated by the root entity (102). The additional entities (104, 106, 108 and 110) may comprise level-one participants and level-two participants. Certificate authorities maintained by level-one participants issue digital certificates that bind the customers to their public keys. System customers are also provided with a warranty request formatter which is adapted to formulate a request for a warranty as to the veracity of information contained in a digital certificate. The warranty request formatter is also adapted to transmit the request for the warranty to the customer's level-one participant. The level-one participants maintain an intelligent messaging gateway which is adapted to receive messages from their customers and to transmit messages to appropriate system entities. Warranty offers are issued by the participant that issued the digital certificate identified in the warranty request. The participants are required to maintain collateral with a collateral custodian.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

SYSTEM AND METHOD FOR PROVIDING CERTIFICATION-RELATED AND OTHER SERVICES

This patent application claims priority from provisional patent application Nos. 60/119,892 and 60/119,958 each of which is hereby incorporated by reference in its entirety. These provisional applications were each filed on February 12, 1999 and entitled: System and Process for Certification in Electronic Commerce. It is believed that no new matter has been added to the disclosure of this patent application beyond that disclosed in the above-referenced provisional applications.

Background of the Invention

The data security market (including hardware) is anticipated to expand to $13.1 billion in sales by the year 2000, up from $6.9 billion in 1997. In addition, the Gartner Group estimates that the market for digital certificates totaled about $100 million in 1998 and will continue to show 100 percent growth in the near term. Soundview Financial recently predicted the certificate market will hit $1 billion in 2001.

Summary of the Invention

Disclosed is a highly secure system for identifying parties over electronic networks, including the Internet. In the disclosed system, member institutions create an entity, referred to hereafter as the root entity, to establish a global, interoperable network of financial institutions which operate as certification authorities. As such, each participating financial institution (each, a "participant") issues digital certificates to customers and corporations and their employees, based on a set of uniform system rules and business practices. The root entity provides the infrastructure within which the system participants provide these services, including establishing technological and procedural systems to support system activities, developing and maintaining rules and regulations governing participation in the system, providing ongoing monitoring and data processing functions to limit the risks to system members and their customers, and establishing a dispute resolution mechanism for issues arising out of use of the system.

The technological, procedural, and legal frameworks established by the root entity and its members permit those members to provide more meaningful and better controlled identity certification services than have previously been available. By doing so, the system encourages the adoption of trusted business-to-business electronic commerce.

The root entity is intended to be a commercially viable, for-profit business that facilitates domestic and international business-to-business electronic commerce by creating a framework for the provision of certification authority services by its participants. Participants use the system to manage the risks involved in acting as certification authorities issuing digital certificates to parties who can then use those certificates to affix digital signatures to messages sent through electronic communications systems, including the Internet. The system is a "closed" system, in which only parties that have agreed to abide by the system's rules and regulations are allowed to participate. The system and its members operate in accordance with a set of operating rules (the "operating rules").

The system is comprised of regulated financial institutions coming together to take the basic technology provided by public key cryptography and public key infrastructure (PKI), and combine it with adherence to a common set of operating rules to facilitate electronic commerce. While the system provides the infrastructure for participating organizations, the service leverages the participants' existing customer base, and the financial institution entity as a trusted financial intermediary. The system is a multi-vendor system, and allows participants to customize the management of identity risk when dealing with individuals over an electronic medium with applications that best meet each particular participant's customer needs.

Participants may join the system either directly, as "Level One Participants" (L1 participants), or indirectly, as "Level Two Participants" (L2 participants). L1 participants may issue certificates either directly to subscribing customers or to L2 participants. L2 participants may issue certificates only directly to subscribing customers. In other respects, the two types of participants operate within the system in the same manner.

The system may be used to facilitate business-to-business e-commerce. The service provided by the system fits well with the needs of mid-size to large institutions for both secure transactions and communications with other businesses.

The disclosed system comprises the following key elements:

1. Risk Management

The system provides an infrastructure for managing risk. The following six, root entity-level key risk areas are analyzed and appropriate controls established within each:

a. Operational

b. Reputation

c. Regulatory

d. Strategic

e. Credit

f. Liquidity/Financial

To further assist with risk mitigation, a "closed" system, as indicated above, is utilized - meaning that both sides of any transaction, are contractually bound to the same set of system rules and operating procedures. From a participant standpoint, the ability to track and monitor outstanding warranties is another feature which also provides the ability to manage risk.

2. Global root certificate authority

The root entity's responsibilities include delivery of the following:

a. root technology.

b. signing keys of all participating financial institutions, which in turn issue certificates to end-users or sign the keys of issuing corporations.

c. establish the infrastructure to facilitate emergence of e-commerce applications, not the applications themselves.

3. Technologically interoperable organization

The system provides a platform for various technologies to "interoperate" with each other.

a. Acting through their participating financial institution, business customers are able to recognize and validate certificates of other business customers.

b. New vendors approach "interoperability" from both a sponsoring and a participating institution standpoint. Technical interoperability is structured in this way to ensure that compliance with technology specifications is equivalent to achieving actual operational interoperability.

c. System interoperability extends beyond technology, to the operating rules, system procedures, and issuance practices of all participants within the system hierarchy.

d. Warranty certificates are used to interact with multiple trading partners, across multiple business applications, in multiple jurisdictions.

4. High trust solution

The trust feature, and benefit from it, is addressed by the system in a number of ways:

a. The system leverages the traditional bank role in identifying customers for purposes of facilitating commerce, and operating as service providers in a regulated environment subject to significant oversight and regulation.

b. The network is dedicated to maintaining high minimum standards.

c. A digital certificate is only as trustworthy as the certifying authority that issued it. The accuracy and validity of a digital certificate is key to a recipient's reliance on a digital signature. By issuing such a digital certificate, the certifying authority certifies the identity of the person sending a message signed with the certificate.

d. Through establishment and compliance with system rules, a PKI is developed that ensures the integrity of the certifying authority's operations.

5. Value-added/unique services offered

As indicated, the system provides numerous security and technical benefits for all institutions involved. Additionally, in several key areas, the system is unique from other current or proposed systems.

a. Validation check

Unlike existing certification systems, the system requires a party to obtain affirmative confirmation of the validity of an identity. The system also provides the means to obtain that confirmation and a warranty thereon on a real-time or near real-time basis through an on-line status check. Thus, while the system and its participants maintain certificate revocation lists ("CRLs") like other systems for control purposes, the system primarily relies on checks of certificates with known "good status" rather than the more customary check of certificates that are known to be bad.

b. Warranty/Assurance (aggregate limits on exposure to identity warranties)

One of the principle functions of the system is to provide warranties and assurances to participants in the network to limit exposure as a result of warranty issuance. Warranty in the system is defined as a warranty of certificate content and validity of certificate at time of issuance. To ensure the viability of these warranties, the system design imposes aggregate limits on the exposure that any issuing participant may incur through explicit warranties granted with respect to identity certificates issued by that institution.

Because each warranty is bounded by the agreements among the parties, both in terms of financial risk and duration, it is possible for each LI participant and the root entity to monitor the participant's compliance with this limit on a real-time basis.

(1) The root entity monitors the cap of all issuing participants on a daily basis. In addition, the system monitors the cap on a real time basis.

(2) The transactions may be captured on a real-time basis, and reported on a periodic basis (to be determined) to the root entity.

(3) The root entity can impose sanctions on participants for violation of warranty cap rules.

(4) The system comprises a mechanism by which to increase or decrease warranty cap.

c. Required collateral posting

To help ensure liquidity for payment of potential warranty assurance claims, collateral is required of all institutions issuing this assurance. The collateral is based on a combination of two criteria:

(1) Credit Based Collateral

An individual participant is required to post a specific amount of collateral in accordance with each participant's specific credit rating. Credit rating is checked on a periodic basis, or whenever revised by a rating firm. (It may take the form of a continuous monitoring of credit rating, leading to changes in collateral happening in concert with changing credit ratings).

(2) Performance Based Collateral

This collateral requirement is designed to lower the requirements for participants that have fewer unresolved claims per warranties outstanding. Calculation methodology is based on prior claims and loss history. The required amount is analyzed periodically.

This methodology has been developed to ensure that the legal "preference" issues are adequately addressed. Note that there is no collateral posting requirement in the system based specifically on claims outstanding.

d. Hardware-based certificates

System participants employ only hardware-based certificates. Relying solely on hardware based certificates differentiates the system from other CA vendors, which all provide software to enable certificate issuance. This point of differentiation strengthens the PKI and reduces operational risk. End-users have smart-card based certificates that employ standard smart-card technology, thus enforcing the same principles of vendor interoperability that the system applies to certificate authority vendors.

Secondary relationships may develop between participants and vendors to assist in the implementation of various applications. However, participants are required to demonstrate that non-system software and hardware is Year 2000 compliant.

e. Shuffled fragmented root key

The ability to provide for shuffled and fragmented root keys is another security feature specific to the system.

Brief Description of the Drawings

The above summary of the invention will be better understood when taken in conjunction with the following detailed description and accompanying drawings, in which:

Fig. 1 is a high level graphic depiction of the system structure;

Fig. 2 is a block diagram illustrating the relationship between the parties in the system operating model;

Figs. 3-7 are a series of conceptual diagrams that illustrate the flow of data through the system for initialization, validation, and warranty processes;

Fig. 8 illustrates aspects of the dispute resolution process of the present system;

Fig. 9 illustrates aspects of the collateral management system of the present system;

Figs. 10-12 illustrate aspects of user interaction with the present system;

Fig. 13 illustrates aspects of the root entity of the present system; and

Fig. 14 illustrates aspects of a participant of the present system.

Detailed Description of the Preferred Embodiments

I. Enterprise structure

Fig. 1 is a high level graphic depiction of the system structure. The system comprises a root entity 102 that is initially formed as a global joint venture of eight founding member

banks 104_1 and a technology partner 104_2. Equity membership is then expanded among regulated financial institutions to achieve a diversity of ownership from all major regions of the globe as well as from other financial industry sectors.

The system further comprises a plurality of L1 participants 106_1, a plurality of corporate clients 108, and a plurality of employees 110 of corporate clients 108. Also part of the system, although not shown in Fig. 1, are a plurality of L2 participants 106_2. L2 participants 106_2 also typically have a plurality of corporate clients 108 which each typically have a plurality of employees 110.

A. Role of Root Entity 102

To facilitate operations of participants 106, root entity 102 creates an infrastructure within which participants 106 provide system services. Specifically, root entity 102 engages in the following functions:

1. Acting as a policy authority, establishing a standardized system and process, operational standards, and risk management requirements.
2. Acting as the root certification authority for the system to provide certification for participants 106, enabling them to certify the identities of their corporate customers.
3. Imposing auditing requirements for monitoring adherence to a set of uniform system rules, contracts, and business practices.
4. Performing a repository function, maintaining a database of the L1 participant certificates and their status, to permit root entity 102 to confirm the validity of a certificate at the request of a participant 106.
5. Performing a monitoring function, measuring each participant 106's aggregate warranty exposure.
6. Acting in an overseer role, monitoring compliance with collateral requirements and the payment of collateral upon a participant 106's default.
7. Assisting with branding and marketing for the system.
8. Establishing a platform for initial efforts.
9. Providing root key technology.
10. Providing technology for initial implementation and testing of the root key.

B. Role of Participants 106

1. In general

While root entity 102 is a for-profit entity, significant revenue opportunities also exist at the individual participant level. By offering add-on electronic services, or by "electronifying" existing customer services, participants 106 compete with each other to attract incremental revenue. Participants 106 also have the right to independently determine products, bundles, and services offered, and fees charged to customers. Root entity 102 does not address the fees that participants106 charge their customers, other than establishing a processing fee for each validation to be paid by one participant to another; there is no interchange fee. This structure enhances the market for participant developed electronic commerce applications, and provides for the transformation of traditional bank products for electronic use. All L1 participants 106_1 are required to act as an issuing participant.

Participants 106 providing the services described above engage in the following activities:

1. Acting as a certification authority, verifying the identity of their customers and issuing digital certificates to those customers.
2. Acting as repository for the digital certificates they issue.
3. Acting as reliance manager for the digital certificates they issue.
4. Responding to requests for confirmation of the validity of digital certificates, and for explicit warranties of confirmations.
5. In the case of an L1 participant 106_1, acting as a certification authority to an L2 participant 106_2 and providing, as agent, reliance manager services to customers on behalf of the L2 participant 106_2.
6. Acting as agent of their customers 108, to obtain confirmation of validity of digital certificates issued by other participants 106, and collect payments from and exercise rights against participants 106 when payments are due as a result of a breached warranty.
7. Provide other related services agreed to by participant 106 and its customer 108.

C. Role of L2 Participants 106_2

Initially, all L2 participants106_2 are also required to be financial institutions. Specific eligibility requirements should be included within the operating rules. The role of an L2 participant106_2 is to issue certificates to its customers 108 and act as principal on warranties

issued. L1 participants 106_1, provide the outsourced reliance manager function to their L2 participants 106_2.

D. Criteria for Participation in the System

The criteria for participation are dependent upon the entity's role as an LI participant 106, L2 participant 106_2, corporation (customer 108), or user (employee 110). In all cases, however, the criteria are designed to:

1. Protect the system and its members from the legal, operational, credit and reputational risks that may arise from the failure of a member to meet its obligations with respect to certificate and warranty issuance and usage.
2. Ensure that the institution is operationally competent to carry out its obligations within the system
3. Ensure that the system complies with all applicable laws

E. Termination of Membership

Participants 106 may be terminated only for specific reasons related to preserving system integrity and favorable risk posture. Procedures provide participants 106 with notice and opportunity to cure deficiencies. However, participants 106 may be suspended on an immediate and a summary basis to preserve system integrity. L2 Participants 106_2 may be suspended or terminated either by an L1 participant 106_1 at request of root entity 102, or by root entity 102 directly (as backstop). Participants 106 may also elect to suspend or terminate membership in the system. Terminated participants 106 are required to take all necessary steps to terminate system-supported services, and to immediately inform their customers 108. Root entity 102 must also be able to invalidate (almost immediately) the subsequent validation of any certificates issued by suspended or terminated participants 106. (The above provisions apply equally to suspended participants 106.)

II. Operational Concepts

A. Operating Model Overview

The system is based on an operating model with five primary parties: root entity 102, an issuing participant 10, a subscribing customer 20, a relying participant 30, and a relying customer 40. The relationship between these parties is illustrated in Fig. 2. Also shown in Fig. 2 is a collateral custodian 112.

Each component depicted in Fig. 2 is certified by root entity 102 and possesses its own certificate, which in turn is validated through a trusted hierarchy. Certificates are issued

to L1 participants 106_1, which then issue their certificates to L2 participants 106_2 or customers 108. The relationships, as depicted in Fig. 2, are: subscribing customer 20 is a customer of issuing participant 10, and relying customer 40 is a customer of relying participant 30. As described in more detail below, each customer 108 interacts with the system through its respective participant 106. In a typical transaction, a seller asks its financial institution (L1 participant) to validate the credentials of a buyer. The seller's financial institution contacts the buyer's financial institution, which in turn attests to the identity of its customer, a buyer. Conversely, if the buyer wishes to check a seller's certificate, the process takes place the same way, with each party relying on a digital certificate and digital signature by first consulting its own financial institution. In addition, as part of the process, the financial institution may offer an identity warranty service for either party, as described in more detail below. In this model, issuing participant 10 is the primary obligor on warranties, while relying participant 30 acts as an agent. Each L1 participant 106 maintains a collateral account with a collateral custodian which is distinct and separate from issuing participant 10, and which will support the warranty issuance capability.

B. Operational Flows

Figs. 3-7 are a series of conceptual diagrams that illustrate the flow of data through the system for initialization, validation, and warranty processes. Fig. 3 is described in this section. Figs. 4-7 are described below.

As shown in Fig. 3, each entity in the operating model of Fig. 2 comprises elements that facilitate the business processes described below. In particular, root entity 102 comprises a certificate authority 302 and a participant repository 304. Certificate authority 302 issues digital certificates to L1 participants 106_1 as described in more detail below.

Issuing participant 10 comprises a certificate authority 306 that is connected to a repository 308. Certificate authority 306 issues digital certificates to customers of issuing participant 10, as described in more detail below. Repository 308 is further connected to an IP certificate risk check and reporting module 310. Issuing participant 10 further comprises bank legacy systems 312, other transaction systems 314, and other tracking DBFs 316. Elements 308-316 are all connected to an intelligent messaging gateway (IMG) router 318 through which flows all messages to and from issuing participant 10 relating to the provision of system services.

Subscribing customer 20 has a digital certificate 322 that it receives from issuing participant 10. Subscribing customer 20 also has the necessary equipment to communicate with relying customer 40.

Relying participant 30 comprises a certificate authority 324 that is connected to a repository 326. Certificate authority 324 issues digital certificates to customers of relying participant 30, as described in more detail below. Repository 326 is further connected to an IP certificate risk meter and reporting module 328. Relying participant 30 further comprises bank legacy systems 330, other transaction systems 332, and other tracking DBFs 334. Elements 326-334 are all connected to an IMG router 336 through which flows all messages to and from relying participant 30 relating to the provision of system services.

Relying customer 40 has a digital certificate 338 and a client IMG formatter 340. Messages from relying customer 40 requesting a system service are formatted by IMG formatter 340 and transmitted to IMG router 336.

C. Proposed Business Process

The operating model is useful in understanding the structure of the system. To better understand the system at work, closer examination of the processes on the front and back-end is required. There are a number of discrete steps that occur within the normal operation of the system.

1. Initialization of L1 participants 106_1

Initialization of L1 participants 106_1 is described in connection with Fig. 4. As shown in Fig. 4, in step A, a prospective L1 participant 106_1 applies for admission to the system. In step B, the applicant receives and signs a participation agreement and agrees to be bound by the operating rules. The prospective L1 participant must agree to act as an issuing participant 10 in order to also act as a relying participant 30. Also in step B, root entity 102 sets a maximum warranty cap for the applicant and a collateral amount that the applicant is required to post. The specific amount of collateral that a participant must post per warranty certificate issued varies from participant to participant based on established criteria - and as discussed below.

Root entity 102 also orients the L1 participant 106_1 and helps establish an implementation schedule. The new L1 participant 106_1 establishes internal certificate authority operation with appropriate testing and sign-off by root entity 102. The new L1 participant 106_1 also opens a collateral account with collateral custodian 112 and deposits

funds as required by root entity 102. Collateral custodian 112 notifies root entity 102 when such funds are transferred by the new L1 participant 106_1 to collateral custodian 112. Collateral custodian 112 provides monthly reports to root entity 102 for each collateral account established at collateral custodian 112.

In step C, the L1 participant 106_1 requests a digital certificate from root entity 102. In step D, root entity 102 issues the requested digital certificate to the L1 participant 106_1. In step E, issuing participant 10 and relying participant 30 execute and exchange an inter L1 contract.

2. Issuance of Certificates

L1 participants 106_1 issue two kinds of certificates - warranty certificates and utility certificates. The utility certificate is merely a technical necessity to facilitate the issuance and usage of the warranty certificate. (The utility certificates should be discussed in more detail in the operating rules. The discussion below deals with usage of warranty certificates.)

The warranty certificate is needed to obtain the validation and warranty assurance services discussed below. Warranty certificate issuance is described in connection with Fig. 5. As shown in Fig. 5, in step 502, subscribing customer 20 requests a certificate from issuing participant 10. In step 504, issuing participant 10 does an appropriate due diligence to ensure that "know your customer" requirements have been met. In addition, a request for a certificate must be authenticated and approved before certificate issuance. In step 506, subscribing customer 20 receives and signs a customer agreement with issuing participant 10 (see also step F in Fig. 4). In step 508, the issuing participant 10 issues the certificate to subscribing customer 20 (see also step G in Fig. 4). Analogous steps are performed to issue a digital certificate to relying customer 40.

3. Requesting an Identification Validation (Warranty Assurance with Zero Value)

Identification validation is described in connection with Fig. 6. It should be noted that all of the following interactions are associated with the warranty certificate and signed transactions.

As shown in Fig. 6, in step A, subscribing customer 20 initiates a transaction with relying customer 40. In step B, relying customer 40 requests an identification validation from relying participant 30.

In step C, relying participant 30 checks with root entity 102 as to the validity of issuing participant 10's certificate. In step D, relying participant 30 receives a response to this check from root entity 102. In step E, relying participant 30 checks with issuing participant 10 as to the validity of subscribing customer 20's certificate. In step F, relying participant 30 receives a response to this check from issuing participant 10. In step G, relying participant 30 forwards the results of these checks to relying customer 40.

4. Requesting an Identification Validation with Warranty

Identification validation with warranty is described in connection with Fig. 7. As shown in Fig. 7, in step 702, subscribing customer 20 initiates a transaction with relying customer 40 (see also A in Fig. 7E). In step 704, relying customer 40 requests an identification validation with warranty from relying participant 30 (see also B in Fig. 7E). The request includes the estimated damages to relying customer 40 if subscribing customer 20 is misidentified and a specified period for which relying customer 40 wants the warranty to be valid.

In step 706, relying participant 30 checks with root entity 102 as to the validity of issuing participant 10's certificate (see also C in Fig. 7E). In step 708, relying participant 30 receives a response to this check from root entity 102 (see also D in Fig. 7E). In step 710, relying participant 30 checks with issuing participant 10 as to the validity of subscribing customer 20's certificate and conveys the warranty request to issuing participant 10 (see also E in Fig. 7E). In step 712, issuing participant 10 checks the validity of subscribing customer 10's certificate and determines whether it will issue a warranty as requested and the cost for such a warranty. Issuing participant 10 may issue the warranty only if the warranty amount would not place the aggregate amount of warranties outstanding of issuing participant 10 over its warranty cap.

If issuing participant 10 declines to issue a warranty, then in step 714, it transmits a message to that effect to relying participant 30. In step 716, relying participant 30 forwards this message to relying customer 40, and this scenario ends. Otherwise, if issuing participant 10 agrees to issue a warranty, then the scenario continues with step 718, in which issuing participant 10 updates its total outstanding issuance against its cap to reflect the new activity, and within required time frames, updates collateral with respect to the formula outlined above (see also J in Fig. 7E). At the end of the day, or as required, issuing participant 10 exports

current status of its warranty cap to root entity 102's Warranty Cap and Collateral Manager (WCCM) which reflects all warranty certificates issuing participant 10 issued that day.

As noted, issuing participant 10 is subject to a warranty issuance limit in total. In addition, however, issuing participants 10 may also choose to establish limits on a per-subscriber basis. This, however, is not a system requirement.

If issuing participant 10 decides to issue the warranty, then, in step 720, issuing participant 10 transmits its acceptance of the warranty request to relying participant 30. This message includes warranty terms and a contract (see F in Fig. 7E). In step 722, relying participant 30 prices the warranty. In step 724, relying participant 30 transmits the terms of the warranty to relying customer 40 (see also G in Fig. 7E). In step 726, relying customer 40 decides whether to purchase the warranty at the price and terms communicated. If relying customer 40 elects to decline the warranty, then in step 728, relying customer 40 declines the warranty and notifies issuing participant 10.

Otherwise, if relying customer 40 elects to accept the warranty, the scenario continues as follows: In step 730, relying customer 40 returns an acceptance of the terms of the warranty to relying participant 30 (liability remains with issuing participant 10). The acceptance includes the signed warranty contract (see H in Fig. 7E). In step 732, relying participant 30 notifies root entity 102 and issuing participant 10, and bills relying customer 40's account for the total fees associated with the warranty (in some cases, subscribing customer 20 is responsible for charges and the billing structure is different). The notification to issuing participant 10 includes the signed warranty contract (see I in Fig. 7E).

Relying participant 30 need not check with root entity 102 as to whether issuing participant 10 is within its limits before the transaction is completed. The reports required by the system inform root entity 102 (independently of issuing participant notification). Those banks over their limits are sanctioned as indicated in this document and the operating rules. In addition controls in the system monitor the limits.

In relation to warranties, if the window is thirty minutes or less between offer and acceptance, a follow-up validation of certificate status (for either issuing participant 10 or subscribing customer 20) is not required. Individual participants 106 may put into place more stringent requirements.

At the end of the day, root entity 102's warranty cap and collateral manager (WCCM) reflects all warranty transactions each issuing participant has issued that period, and issues a

revised aggregate position to the participant 106 and root entity 102. The additional collateral is posted and transferred to the collateral account trustee. The WCCM does an end of period assessment to determine new level of collateral based on market changes.

To ensure that the system can accurately bill for these validation and warranty services, a system accounting mechanism for tracking must be in place. Only one issued warranty is allowed per transaction (for duration of that warranty). Only one bid can be issued (outstanding) per transaction at a time. This must be acted against before another bid is placed. The amount of the outstanding bid must be "reserved" against the warranty limit. Relying participant 30 can refuse to request a validation or Identity Warranty Assurance (IWA) from issuing participant 10 if legally prohibited from doing so (e.g. to comply with OFAC).

If one bank is both an Issuing and Relying Participant in a particular transaction, there is:

- No processing fee between banks
- No validation fee to root entity 102
- Still the application of warranty cap and collateral limits (from a warranty assurance standpoint)

5. Claims Processing Business Process

While the system provides for a claim review process to avoid disputes, if standards are adhered to, initiation of claims should be a relatively infrequent occurrence. However, in the event a transaction goes awry as a result of misidentified parties, the system is prepared to handle these situations, should they arise. It is also worth noting that these steps take place outside the normal range of activities, and are not a part of the standard operating flow.

The claims processing business process is described in connection with Fig. 8. As shown in Fig. 8, after a warranty is issued to a relying customer 40 (step 802), one of the following occurs:

- Relying customer 40 files a claim within the warranty expiration date (step 804, see also B in Fig. 8F);
- Relying customer 40 does not file a claim within the applicable time period and the warranty expires (step 806); or

- Relying customer 40 files a claim after the applicable time period and the warranty expires (step 808).

If, as depicted in step 804, relying customer 40 files a claim within the warranty time limit (along with associated supporting evidence) with relying participant 30, then the system proceeds to step 810 where relying participant 30 notifies the corresponding issuing participant 10 of a filed claim and provides supporting evidence per the contractual obligations with the issuing participant 10 and relying customer 40 (see also C in Fig. 8F).

In step 812, relying participant 30 notifies both root entity 102, and issuing participant 10's WCCM of the filed claim and the amount of claim. In step 814, issuing participant 10 determines whether it will pay. Root entity 102 sets conditions under which claims against warranties shall be paid. The intent is to make sure there is a gold standard for business. Each warranty issuer is provided the latitude to evaluate and dispose of claims using its own procedures. However, minimum standard criteria are established under which claims would be paid.

If issuing participant 10 decides not to pay the claim, the system branches to step 816 where issuing participant 10 informs relying participant 30 of its decision.

In decision step 818, if relying customer 40 is dissatisfied with issuing participant 10's decision, then the system branches to step 820 where relying customer 40 may initiate dispute resolution/arbitration proceedings (see also E in Fig. 8F). In that event, the collateral is only "released" after the outcome of the dispute resolution process.

It should be noted that, relying participant 30 may provide a provisional credit/credit enhancement to relying customer 40 in its discretion; if so, relying participant 30 pays relying customer 40 before issuing participant 10 agrees to cover the claim and subrogation allows relying participant 30 to file claim with issuing participant 10, subject to contracts specifying this right. If relying participant 30 provides a credit enhancement to relying customer 40, relying participant 30 is not be required to post collateral as a result.

If (in step 814) issuing participant 10 decides to pay the warranty claim, then the system branches to step 822 where issuing participant 10 informs relying participant 30 of its decision. In step 824, issuing participant 10 pays the claim to relying participant 30 (see also D in Fig. 8F). In step 826, the WCCM monitors the fact that issuing participant 10 has paid the claim, decreases the amount of collateral by amount paid, and also by amount required.

If, as depicted in step 806, a claim is not filed within the warranty expiration date, then the system proceeds to step 828 where the warranty expires. In step 830, issuing participant 10's outstanding warranty amount is decreased by the expired warranty amount. In step 832, at the end of the day, root entity 102's WCCM decreases the collateral requirement to reflect expiration of warranties.

If, as depicted in step 808, a claim is filed after warranty expiration, then the process is the same as if a claim was not filed except that the full value of the outstanding warranty is now reflected back in the WCCM.

6. Collateral Management

As mentioned above, each L1 participant 106_1 must post collateral in accordance with the criteria established by root entity 102 to be eligible to issue warranty certificates. The following are a number of guidelines regarding collateral posting:

1. Root entity 102 is agent for collateral and can direct the collateral trustee to pay relying customer 40.

2. If an issuing participant 10 fails, root entity 102 does not pay valid IWA claims exceeding available collateral.

3. If an issuing participant 10 fails, competing claims are paid on a "first-come, first-served" basis.

4. If an issuing participant 10 fails, and collateral is not readily accessible, root entity 102 does not advance funds.

5. If a participant 106 is terminated, it must post 100% of anticipated claims, based on historical experience for the warranties outstanding.

6. Root entity 102 determines required collateral of each participant 106 daily; collateral amounts are assigned "haircuts," emulating the CHIPS model.

7. Root entity 102 receives frequent reports from participants 106 on IWAs approved and IWA claims filed to determine collateral required.

The collateral management system is further described in connection with Fig. 9. As shown in Fig. 9, the collateral management system comprises a collateral custodian or trustee 112 which maintains custodial accounts 902 for a plurality of participants 106 and whose activities are monitored by root entity 102. The sizes of the custodial accounts are indicated by the grey areas labeled C1-6 in Fig. 9. As Fig. 9 further demonstrates, the collateral

requirement is typically less than the total value of outstanding warranties that have been issued by a participant 106, but the percentage is variable, rather than fixed.

Also shown in Fig. 9 is an embodiment for calculating the collateral requirement for a particular participant. For purposes of the illustrated embodiment, it is assumed that the total outstanding warranty values for a particular participant 106 is $50M. The collateral requirement for the participant 106 is then calculated as follows in the illustrated embodiment:

Requirement = $1M
+ value of outstanding claims made by system customers
+ the total amount of outstanding warranties issued by participant 106 to its top three customers
+ 3% of the total amount of outstanding warranties issued by participant 106

Thus, assuming for purposes of the illustrated embodiment that the value of claims outstanding against the participant 106 by system customers is $0.5M, the total amount of outstanding warranties issued by participant 106 to its top three customers is $4M, and 3% of the total amount of outstanding warranties issued by participant 106 is $1M, then the total collateral requirement for the participant 106 in the illustrated embodiment would be $6.5M.

7. End-User Experience

The end user is usually an employee 110 of a corporation 108 that has signed a contract with a participant 106 to use the system service. The components available to employee 110 for use with the system are shown in Fig. 10. As shown in Fig. 10, employee 110 is given a certificate on a smart card 1002 by employer 108 or participant 106. Employee 110 also has a smart card reader 1004 attached to his PC 1006 which has installed any necessary software 1008 to use smart card reader 1004. Employee 110 must also load system-enabled application software 1010 on to his desktop 1006 or access it through a browser to a server (not shown). The location of application software 1010 should be transparent to employee 110.

Depending on whether the end user is acting as a subscribing customer 20 or a relying customer 40, interaction with the system will vary. End user interaction is also a function of the application and relying customer 40's requirements. Therefore, this narrative serves as an

example of how an end user interacts with a system application and the types of messages and procedures the end user follows.

An illustrative example of a system interaction is now described in connection with Fig. 11. For purposes of this example, assume that the end user is a purchasing manager of an entity desiring to purchase office supplies (an employee 110 of a subscribing customer 108) and relying customer 40 is an entity that sells office supplies (referred to as the "seller"). In step 1102, employee 110 starts up his web browser and goes to the site of relying customer 40. In step 1104, employee 110 interacts with the web site, selecting, for example, the supplies he needs. He could also conduct other transactions such as submitting an RFP, placing an order, negotiating a contract, etc. When employee 110 is ready to complete the transaction, he indicates this to the system (step 1106). For example, employee 110 may click on a button to indicate that he is ready to submit his order and purchase the supplies. In step 1108, the seller's system may ask employee 110 for other information needed to complete the order, such as ship-to address. In step 1110, employee 110 is then asked to insert his smart card into the reader. Employee 110 places his smart card into the reader and enters his PIN. If the PIN is valid, then in step 1112, the user sees a message saying the system is processing his transaction.

In step 1114, the employee 110's system software 1010 signs the transaction and sends it with his warranty certificate to relying party 40, in this case the seller. In step 1116, relying party 40 then validates the buyer's certificate by sending a message to relying participant 30. In step 1118, relying participant 30 sends a message to issuing participant 10 to determine if the certificate is valid, as explained above. In step 1120, issuing participant 10 sends a response back to relying participant 30 that says the buyer's certificate is valid. Issuing participant 10 also includes its own certificate in the response. In step 1122, relying participant 30 then sends a message to root entity 102 to determine if issuing participant 10's certificate is valid. If all of these responses are yes, then in step 1124, the seller sends a message back to employee 110 that his transaction has been accepted, along with any other pertinent information. The seller's system may have the capability to request an IWA programmed into its software. In this case, the warranty is requested and negotiated in the background (as described above) while the buyer waits for confirmation of his purchase order.

If problems are encountered as the transaction is conducted, appropriate error messages are displayed to employee 110. These include asking employee 110 to reenter his PIN if it was incorrect. Employee 110 is allowed three tries before he is locked out and instructed to see his business manager to re-activate the card. Note: the number of tries before a user's card is disabled may vary depending on the limits set by issuing participant 10.

Employee 110 also has the opportunity to perform an identity verification of the seller. The steps in this process are described in connection with Fig. 12. As shown in Fig. 12, in this case, subscribing customer 10 becomes the relying party and requests the seller to send its warranty certificate (step 1202). The steps then followed are similar to those described above. However, the IWA is not negotiated in the background, but between employee 110, its participant 106, and the seller's participant 106. In step 1204, employee 110 enters the amount and time period for the warranty. In step 1206, this message is sent to issuing participant 10 which sends it to the seller's ("relying") participant 30. In step 1208, employee 110 gets a message back saying the warranty request was accepted and the fee for the IWA. In step 1210, employee 110 decides if the warranty terms are acceptable. If employee 110 agrees to pay the specified amount, the system branches to step 1212 where employee 110 sends this response through issuing participant 10 to the seller's ("relying") participant 30. If, however, employee 110 does not want to pay the charge for the IWA, the system branches to step 1214 where employee 110 sends a message back, either declining the IWA or requesting another IWA for a different date and amount. This negotiation continues until employee 110 either accepts the IWA and the associated fee or says no and ends the transaction.

All transactions are logged so that in the event of disputes or questions, employee 110, issuing participant 10, root entity 102, relying party 40, and relying participant 40 can refer to this information.

III. Roles and Responsibilities

Each entity in the operating model shown in Fig. 2 bears certain roles and responsibilities within the system. These roles and responsibilities are summarized below.

A. Root Entity 102

Root entity102 sits atop the operating model, serving as the main "backbone" for the system. It performs the following critical functions to facilitate seamless operation of the system:

1. Operates a root level repository to provide on-line status for validity of L1 participant certificates.
2. Sets and establishes rules and standards constraining operations of all subordinate entities.
3. Identifies prospective L1 participants 106.
4. Qualifies L1 participants for admittance based on criteria established in rules.
5. Conducts due diligence on prospective L1 participants as part of chartering process.
6. Evaluates a prospective L1 participant's technology for fit with system standards prior to charter.
7. Defines limitations associated with each L1 participant's operation as a certificate authority or reliance manager (Note: when "reliance manager" is used it refers to the operations related to the issuance verification and settlement of the warranty product.).
8. Establishes warranty cap on total aggregate outstanding warranty (in the event that an L1 participant 106 acts as a reliance manager).
9. Executes L1 participation agreements.
10. Collects fees for:
   - Chartering a certificate authority, reliance manager;
   - Recurring annual membership fees;
   - Issuing certificates to L1 participants 106 (or other customers);
   - Validation transactions;
   - Percentage of warranty issuance costs;

To ensure the system can accurately bill for these services, the reliance manager must have an accounting system.

11. Monitors L1 participant 106 operations for:
   - Compliance with system standards;
   - Warranty issuance activity.
12. Reviews independently conducted audits of subordinate activities.

13. Reserves the right to conduct its own audit of subordinate activities and to intervene in subordinates activities that are non-compliant or excessively risky.
14. Maintains system risk reserve - provides reserve in the form of LC or other guarantees to provide vehicle for managing risk resulting from system failure for which root entity 102 assumes liability.

As noted, root entity 102 is responsible for managing the root operation and maintaining the integrity of the system. The root functions are performed either centrally or distributed, depending on what the function is. The entities within root entity 102 that are responsible for performing these functions are now described in connection with Fig. 13.

As shown in Fig. 13, root entity 102 employs a private key made up of five root key fragments 1302. Each fragment 1302 is stored on its own token 1304 which is kept secured when it is not being used by a key fragment holder 1306.

Each key fragment holder 1306 is responsible for the security of his fragment 1302 and for presenting fragment 1302 to a signing device host 1308 when needed for the approval of certificate authority transactions such as issuance of certificates and CRLs. In particular, when, for example, a certificate is to be signed, key fragment holder 1306 is present to input his token into a signing device host 1308.

- Suggested level: Vice President or equivalent

Key fragment holders 1306 and signing device hosts 1308 are located in geographically diverse locations. The distribution of key fragments 1302 provides a high level of security and protection for the root private key. As further shown in Fig. 13, two key fragment holders 1306 and signing device hosts 1308 are located in a data center 1310 in New York (one PC, one reader, and two tokens), two in a first bank data center 1312 in Frankfurt, Germany (one PC, one reader, and two tokens), and the fifth in a second bank data center 1314 in Hong Kong.

Also shown in Fig. 13 are signing officer stations 1316 that are geographically disbursed as well, with one located at each founding bank 104_1 for a total of eight signing officer stations 1316. Signing officer stations 1316 are located in a secure location at each of the founding members 104_1.

Each bank 104_1 also has two signing officers (SOs) 1318 for a total of 16 altogether. Signing officers 1318 are responsible for operating signing officer workstations 1316. Each founding bank 104_1 may, if desired, have a back-up for each SO 1318. Each SO 1318

approves the use of his/her fragment to generate the root key to sign certificates, revocations, CRL's, and SO changes based upon verification of request data and based upon a recommendation from an authorizer 1320, described below. SO 1318 does not directly sign a certificate.

- Suggested level: Vice President or equivalent

The certificate signing process works on the basis of quorums. A quorum of SOs 1318 is needed to approve the use of a fragment 1302 before it can be "released" to the root key generation algorithm. A quorum of fragments 1302 must be approved to generate the root key to sign the certificate. Quorums are established at the time the key is generated. One reject/no vote rejects the whole request.

Authorizer 1320 is also shown in Fig. 13. The function of authorizer 1320 resides at founding banks 104_1. While this is a required function, it may not necessarily require a dedicated resource. Authorizer 1320 receives and reviews the documentation for root certificate requests, revocations, CRL's, SO maintenance, etc. This person makes the recommendation to SOs 1318 to approve or reject the requests that have been received, and is responsible for ensuring that SOs 1318 have access to documentation (e.g. meeting notes) to facilitate sound decision-making. If sufficient information is unavailable to approve the request, it must be rejected.

- Suggested level: Vice President or higher

Also shown in Fig. 13 is a registrar 1322. Registrar 1322 is a root entity 102 employee. This person receives and reviews the documentation for CA transactions such as certificate and CRL requests, and then inputs the request into a CA 1324, initiating the signing process.

- Suggested level: Officer or equivalent

Also shown in Fig. 13 is a system administrator 1326. System administrator 1326 is a root entity 102 employee who manages the system and its databases by doing functions such as:

a) Defining and maintaining information about issuers, SOs 1314, and registration authorities 1328

b) Performing backups

c) Changing passwords

- Suggested level: Officer or equivalent

Also shown in Fig. 13 is a root CA auditor 1330. Root CA auditor 1330 is responsible for reviewing CA 1324 and SO 1318 records to ensure that the PKI has not been compromised and procedures are being followed. This review entails verifying the audit records, validating the information in the audit records, and making sure that none are missing. Root CA auditor 1330 must also examine the key pairs submitted for certification, and resulting digital signatures for authenticity before it is released for use. This individual should be within the operations area and differs from those designated within the risk management area of root entity 102.

- Suggested level: Vice President or equivalent

The Root CA 1324 is kept in a highly secure location, with physical and virtual access controls to ensure the system cannot be intruded upon. To minimize the risk of a root key compromise, the root key is never maintained as a whole, but rather in 5 fragments. Three of these 5 fragments constitute a "quorum", or the number of fragments to be used in the mathematical formula that recalculates the root key every time it is needed for a signing operation. The quorum rules are:

a) The fragment quorum is 3 of 5.
b) An SO can be an SO on no more than 2 fragments.
c) It must be possible to sign if 4 SO's are unavailable.
d) A majority of banks (5 of 8) must approve a certificate, CRL, or administrative change request.
e) Even if SO's from 4 banks cooperated, it must still be impossible to approve a certificate. For security purposes, the SO private keys are maintained on hardware tokens that require 12 digit passwords to access the token.

B. L1 Participants 106_1

Following are the various functions performed by L1 participants 106_1:

1. Operate certificate authority and associated repository.
2. Operate a reliance manager if application to be chartered to be a reliance manager is approved by root entity 102.
3. Optionally issue warranties on veracity of information contained in certificates it issues.
4. Identify and charter L2 participants 106_2.
5. Issue certificates directly to L2 participants 106_2.

6. Administer contractual relationships between root entity 102 and participants 106 subordinate to itself (While an L1 participant 106_1 must act as an issuing participant 10, it need not necessarily act as a reliance manager).

7. Obtain 3rd party audit for compliance with system standards.

8. Report results of audit to root entity 102.

9. Take remedial action as result of root entity 102 review to maintain compliance.

10. Acquire, qualify, and deploy technical components required for L1 participant 106_1 to establish either certificate authority or reliance manager operations.

- Qualification will be against standards set by root entity 102

11. Respond to requests for on-line certificate validation and/or warranties from:

- subscribing customers 20 or peer L1 participants 106_1.

12. Track changes in status of its total warranty exposure.

- L 1 is also responsible for reporting warranty status to root entity 102

13. Maintain adequate levels of collateral for warranties issued.

- responsibility for reporting collateral status to root entity 102

14. Promulgate system's minimum rules, standards, and contract terms to L2 participants 106_2. L1 participants 106_1 have the latitude to define more restrictive standards and rules provided they do not conflict with system standards.

The functions performed by L1 participant 106_1's certificate authority level are similar to those done by the root certificate authority operated by root entity 102. However, the actual roles and responsibilities may be different from those of root entity 102, depending on how each L1 participant 106_1 chooses to implement their certificate authority, including whether or not to use fragmentation for its private key. In addition, the roles described below may vary from participant to participant. One example of the entities within an L1 participant 106_1 that are responsible for performing these functions are now described in connection with Fig. 14.

Shown in Fig. 14 is a registrar 1402 who is the person responsible for inputting the certificate request into the system. This may be done directly by a customer, by an account officer, or by a data entry person.

- Suggested level (if done by bank): Officer or equivalent

Also shown in Fig. 14 is an authorizer 1404. Authorizer 1404 receives from a customer 108 or an account officer the documentation for certificate requests, revocations,

CRL's, SO maintenance, etc. He/she reviews the documentation and makes the recommendation to the signing officer 1406, described below, to approve or reject any of the requests that he/she has received. If he/she has does not have enough information to approve the request, it should be rejected.

- Suggested level: Vice President or equivalent

Also shown in Fig. 14 is a signing officer (SO) 1406 who is responsible for operating a signing officer workstation 1408. Based upon authorizer 1404's recommendation, and verification of the request data, SO 1406 approves the use of L1 participant 106_1's private key to sign certificates, revocations, CRL's, and SO changes. If a bank chooses to fragment their private key, then multiple SO's and quorums are necessary. Each L1 participant 106_1 develops their own procedures to operate this capability.

- Suggested level: Vice President or equivalent

Also shown in Fig. 14 is a system administrator 1410. System administrator 1410 manages L1 participant 106_1's system and databases by performing functions such as:

a) Defining and maintaining information about certificates

b) Performing backups

c) Changing passwords

- Suggested level: Officer or equivalent

Also shown in Fig. 14 is an auditor 1412. Auditor 1412 is responsible for reviewing the certificate authority and SO records to ensure that the PKI has not been compromised and procedures are being followed. This entails verifying the audit records, validating the information in the audit records and making sure that none are missing. Auditor 1412 must also examine the key pairs and digital signatures for authenticity.

- Suggested level: Vice President or equivalent

Each Level 1 certificate authority has its own set of operational and security procedures to be followed. At a minimum, they meet the requirements specified in the system operating rules. Each Level 1 certificate authority has haves its own risk management policies and procedures. At a minimum, they meet the requirements specified in the system operating rules.

C. Customers 108

The responsibilities of system customers 108 are as follows:

1. Enter into an agreement to abide by participant 106's operating rules.

2. Store private keys associated with warranty certificates in a hardware device that complies with system specifications (smart card, HSM) and when used by individuals, to require positive authentication (e.g. PIN entry) for each transaction. [note: the requirement for per-transaction PIN entry/authorization does not apply to server based implementations.] Private keys associated with utility certificates must be stored in hardware devices compliant with system specifications; but do not require explicit authentication on each use.
3. Provide timely and accurate notice to its issuing participant 10 of information relating to ongoing validity and accuracy of its private key/public key pair and identification certificate, or any compromise or suspected compromise of the security of its computer systems or smart cards on which its private key is stored.
4. Obtain written consent from each person or entity authorized to create a digital certificate or named in a digital certificate that information about their person and authority may be transferred to other participants 106 and root entity 102 for the purpose of providing system services or otherwise carrying out the goals of the system.

IV. Risk Management

A. Risk Management System and Infrastructure

Root entity 102 is responsible for establishing a system of risk management within the system infrastructure. Management of each system entity is then responsible for ensuring the appropriate controls and structure are operating effectively. To accomplish this, all participants 106 adhere to a clearly defined set of system rules that are structured to reflect the requirements resulting from the detailed analysis of risks, and the identification of controls appropriate to mitigate those risks. Clearly defined contracts are adopted for binding all parties to these rules.

Various other elements assist with the management of risk. These include:

- Contractual limiting of liability.
- Establishment of minimum criteria for system participation eligibility.
- Ability of root entity 102 to enforce against those participants 106 in non-compliance with their contractual requirements or the standards/procedures established.

- Establishment of a risk reserve and purchase of insurance to protect the entity against system risk.
- Required posting of collateral by those institutions offering the assurance feature
- Monitoring capabilities.

From an administrative standpoint, the risk management function reports to the CEO of root entity 102 - either within the CEO function or as a standalone position. However, it must have direct accessibility to the audit committee.

Root entity 102's risk management policy is to both limit risk and to place responsibility and liability at the point where the risk arises. Therefore root entity 102's risk is limited to the technology and operations directly managed by, or on behalf of, root entity 102. An independent review is performed of the identified risks and proposed controls to assist in the quantification of risk exposure, and the impact and likelihood of loss within the system.

A detailed risk analysis is completed that addresses, in greater detail, the following defined risks and control objectives necessary for their mitigation. Specific controls relevant to each function are then developed, reflected within the appropriate standards, and implemented throughout the system.

B. Risks and Control Objectives

The following six key risks are analyzed by root entity 102 shortly after its formation and then on an ongoing basis.

1. Operational Risks

a) Technology- security breaches or other failures arising from design weakness or misuse of technology supporting the system, which result in system interruptions, cryptographic weaknesses, hardware/application failure.

- Control Objectives: - utilization of expertise in design and implementation, adequate testing before implementation, contingency plans, establishment of security/access policies and controls, independent audits, ongoing monitoring.

b) Processing - all failures in actions through error, design weakness, or inadequate policy and procedure implementation resulting in failure to safeguard keys, untimely or inaccurate processing of certificates/updating CRLs, inappropriate certificate usage, or unauthorized transactions.

- Control Objectives: establishment of operating policies and procedures; establishment of limits, ongoing evaluation of risks, ongoing review/monitoring,

contingency plans, mechanism to monitor limits/risks related to outside service providers, ability to push down requirement for similar controls to the CA,

c) Criminal/Illicit Acts - deliberate attempts to/breaches of the technology in processing within the system and/or the failure to detect the occurrence of fraud, resulting in compromise of keys, misuse of certificates, alteration/theft of data, assumption or forged identifications.

- Control Objectives: processing controls, limits, implementation of security, access measures, regular reviews, and ongoing monitoring for adherence.

2. Reputation Risks - negative impact on public opinion and trust by events or publicity resulting in loss of revenue and/or legal action.

- Control Objectives: ability at the root entity 102 level to promptly act to correct or address failures in operations, security, privacy requirements or compliance related to certificates/usage, enforcement against those CA's or service providers who do not perform in accordance with contract, policy terms, and obligations.

3. Regulatory/Legal Risks - requirements are not adhered to or rules are ambiguous and untested - resulting in fines, penalties, or public embarrassment.

- Control Objectives: establishment of a legal function within root entity 102, agreement requirements that CA's adhere to appropriate laws and regulations, clearly defined rights, obligations, and assumptions of liability within contractual agreements, establishment of ongoing regulatory dialogue.

4. Strategic Risks - failure of market to emerge, competitive edge ceases, expected technology does not occur, or legal and regulatory changes occur which negatively impact the system's product or ability to market.

- Control Objectives: root entity 102 tracking of market, legal, and technology events to enable prompt corrective action, contract limits on financial liability.

5. Credit Risks - failures within the CA's and sub CA's which roll up to, or impact root entity 102.

- Control Objectives: OTO approval of CA members based on certain financial criteria, root entity 102 establishment of caps for each CA, tracking of assurance transactions, claims, and settlements, requirement that CA's establish and adhere to appropriate procedures related to: adherence to limits, knowing your customer requirements, monitoring credit/financial conditions.

6. Liquidity/Financial Risks - adverse or improper business decisions or implementation, inadequately capitalized structure, or insufficient loss protection resulting in serious negative impacts on earnings or capital.

- Control Objectives: strong board, project management, and plan implementation and support of senior management within the banks, hiring appropriate expertise into root entity 102 organization, maintenance of adequate reserves and liability insurance at root entity 102 level; requirement that adequate reserves, and collateral be maintained at the CA level, and establishment of the following at root entity 102 level: financial monitoring, mechanism to address need for additional capital, contract limits on liability.

C. Auditing Requirements

Root entity 102 requires periodic external audits be performed of its own operations as well as those of its members. Member reviews are performed at the member's own expense. Root entity 102 also requires that third party technical reviews be performed periodically. All participants 106, as well as root entity 102, are also required to implement internal risk monitoring programs and routines, which specifically address the risks of their operational functions.

Root entity 102 reserves the right to request/review audit reports and to evaluate, or further test, to ensure that audit corrections have been made. Root entity 102 also reserves the right to, at its own expense, perform or cause to have performed, any additional audit work considered necessary.

While the invention has been described in conjunction with specific embodiments, it is evident that numerous alternatives, modifications, and variations will be apparent to those skilled in the art in light of the foregoing description.

Claims

1. A system for warranting the identity of a party over an electronic network, comprising:

a root entity;

a plurality of additional entities, each additional entity being admitted to the system after agreeing to abide by a plurality of operating rules promulgated by the root entity;

the plurality of additional entities comprising a first level-one participant and a second level-one participant;

a first certificate authority maintained by the first level-one participant and adapted to issue a first digital certificate to a first customer, the first customer being a customer of the first level-one participant, the digital certificate binding the first customer to a first public key;

a second customer, the second customer being a customer of the second level-one participant;

a warranty request formatter maintained by the second customer and adapted to formulate a request for a warranty from the first level-one participant as to the veracity of information contained in the first digital certificate, the warranty request formatter being adapted to transmit the request for the warranty to the second level-one participant;

a first intelligent messaging gateway maintained by the second level-one participant adapted to receive the warranty request and forward the request to the first level-one participant;

a second intelligent messaging gateway maintained by the first level-one participant adapted to transmit a warranty offer to the first intelligent messaging gateway, the warranty offer constituting a promise by the first level-one participant to pay money to the second customer if information in the first digital certificate is incorrect.

2. The system of claim 1, wherein the warranty further includes a promise by the first level-one participant to pay money to the second customer if a signed message received by the second customer was not authorized by the first customer.

3. The system of claim 1, further comprising:

a second certificate authority maintained by the second level-one participant and adapted to issue a second digital certificate to the second customer, wherein the warranty request transmitted to the intelligent messaging gateway of the second level-one participant includes the second digital certificate.

4. The system of claim 3, further comprising:

a third certificate authority maintained by the root entity and adapted to issue a digital certificate to each additional entity, wherein the warranty request forwarded to the intelligent messaging gateway of the first level-one participant includes the digital certificate of the second level-one participant.

5. The system of claim 1, wherein the additional entities comprise a level-two participant.

6. The system of claim 1, further comprising a collateral custodian, the collateral custodian maintaining a collateral account for the first level-one participant.

7. The system of claim 6, wherein the first level-one participant is required to maintain a minimum balance in the collateral account.

8. The system of claim 7, wherein the minimum balance is a function of the warranties that the first level-one participant has issued.

9. The system of claim 7, wherein the minimum balance is a function of the amount of warranties that the first level-one participant has issued to a subset of its customers.

10. The system of claim 9, wherein the subset is the three customers as to whose digital certificates the first level-one participant has issued the most warranties in dollars.

11. The system of claim 7, wherein the minimum balance is a function of the total amount of outstanding warranties issued by the first level-one participant.

12. The system of claim 7, wherein the minimum balance is a function of value of outstanding claims made by system customers against the first level-one participant.

13. The system of claim 7, wherein a portion of the minimum balance is a fixed amount.

14. A method of warranting the identify of an individual within the context of a certificate authority system, the system comprising a root certificate authority, the root certificate authority adapted to issue a first certificate to an issuing participant and a second certificate to a relying participant; the issuing participant adapted to issue a third certificate to a subscribing party; the relying participant adapted to issue a fourth certificate to a relying party; comprising:

transmitting first information from the subscribing party to the relying party, the first information comprising transaction information, the third certificate, and the first certificate;

transmitting second information from the relying party to the relying participant, the second information comprising a request for a warranty as to the identity of the entity named in the third certificate and the fourth certificate, the request for warranty constituting a request for a binding promise from the issuing participant to the relying party to pay damages or submit to arbitration if the entity named in the third certificate did not authorize the digital signature;

transmitting third information from the relying participant to the issuing participant, the third information comprising a request for the warranty and the second certificate;

at the issuing participant, determining whether to issue the warranty, the step of determining comprising the step of determining whether the requested warranty would cause the issuing participant to exceed one of the issuing participant's warranty cap or collateral cap;

transmitting fourth information from the issuing participant to the relying participant, the fourth information comprising an offer to issue the warranty to the relying party;

transmitting fifth information from the relying participant to the relying party, the fifth information comprising the offer to issue the warranty to the relying party;

transmitting sixth information from the relying party to the relying participant, the sixth information comprising an acceptance of the offer;

transmitting seventh information from the relying participant to the issuing participant, the seventh information comprising the acceptance of the offer;

whereby a warranty is established in which the promisor is the issuing participant and the promisee is the relying party.

15. The system of claim 14, wherein the relying party has no recourse against the issuing participant unless the warranty is established.

16. A system for providing a plurality of services over a closed network comprising:

a root entity;

at lease one issuing participant;

at least one relying participant;

at least one relying customer;

wherein one of the plurality of services is a warranty from the issuing participant to the relying customer and wherein each of the plurality of services is made available to the relying customer via the relying participant.

17. A system for providing a plurality of services over a closed network comprising:

a root entity;

at least one level one participant;

at least one level two participant, the level two participant acting as a relying participant with respect to its customers;

at least one relying customer, the relying customer being a customer of the level two participant, wherein each of the plurality of services is made available to the relying customer via the level two participant.

18. A system for providing dispute resolution to entities belonging to a closed network, comprising:

a root entity;

at lease one issuing participant;

at least one relying participant;

at least one relying customer, wherein the relying customer transmits messages relating to a dispute with the issuing participant via the relying participant.

19. A system for providing certificate warranties over a closed network comprising:

a root entity;

at lease one issuing participant , the issuing participant being required to post collateral with a collateral custodian in accordance with requirements established by the root entity, the amount of the collateral being based on the issuing participant's credit rating and the issuing participants prior claim and loss history;

at least one relying participant;

at least one relying customer, the relying customer receiving a certificate warranty from the issuing participant;

20. The system of claim 19, wherein the root entity may direct the collateral custodian to pay the relying customer.

21. The system of claim 19, wherein the root entity is not responsible to pay valid claims made by relying customers in the that exceed the available collateral.

22. The system of claim 19, wherein the root entity pays valid claims made by relying customers on a first-come, first-served basis.

23. The system of claim 19, wherein if the issuing participant is terminated, the issuing participant must post collateral covering all anticipated claims, based on historical experience for the warranties outstanding.

24. The system of claim 19, wherein the root entity determines the required collateral of each participant daily.

25. The system of claim 19, wherein the root entity receives frequent reports from participants on warranties approved claims filed.

26. A method for initializing a level one participant for providing a plurality of services over a closed network comprising the following steps:

applying for admission to the network;

agreeing to be bound by the network rules;

agreeing to act as an issuing participant before being permitted to act also as a relying participant;

receiving a maximum warranty cap from the root entity;

establishing an internal certificate authority;

opening a collateral account with a collateral custodian;

depositing the amount of collateral in a collateral account;

requesting a digital certificate from the root entity; and

receiving a digital certificate from the root entity.

27. A method for providing an identity warranty service over a closed network comprising the following steps:

a subscribing customer initiating a transaction with a relying customer;

the relying customer requesting an identification validation with warranty from the relying participant;

the relying participant checking with a root entity as to the validity of an issuing participant's certificate;

the relying participant receiving a response to the check from the root entity;

the relying participant checking with the issuing participant as to the validity of the subscribing customer's certificate;

the relying participant conveying the warranty request to the issuing participant;

the issuing participant checking the validity of the subscribing customer's certificate;

if the issuing participant decides not to issue the warranty:

the issuing participant transmitting a negative message to the relying participant;

the relying participant forwarding the message to the relying customer; and

if the issuing participant decides to issue the warranty:

the issuing participant updating its total outstanding issuance against its warranty cap;

the issuing participant updating its collateral;

the issuing participant reporting the status of its warranty cap to the root entity and the collateral custodian;

the issuing participant transmitting its acceptance of the warranty request to relying participant;

the relying participant pricing the warranty;

the relying participant transmitting the terms of the warranty to the relying customer;

if the relying customer decides not to purchase the warranty at the price and terms communicated:

the relying customer notifying the issuing participant; and

if the relying customer decides to purchase the warranty at the price and terms communicated:

the relying customer returning an acceptance of the terms of the warranty to the relying participant; and

the relying participant notifying the root entity and the issuing participant; and

the relying participant billing the relying customer's account for the warranty price.

28. A method for providing dispute resolution over a closed network comprising the following steps:

a relying customer filing a claim with a relying participant;

the relying participant notifying an issuing participant, a root entity, and a collateral custodian of the filed claim and the amount of claim;

if the issuing participant decides not to pay the claim:

the issuing participant informing the relying participant of its decision not to pay the claim;

initiating a dispute resolution proceeding if the relying customer is dissatisfied with the issuing participant's decision;

if the issuing participant decides to pay the claim:

the issuing participant informing the relying participant of the decision;

the issuing participant paying the claim to the relying customer;

the collateral custodian monitoring that the issuing participant has paid the claim, and decreasing the amount of collateral by the amount paid and also by the amount of the claim.

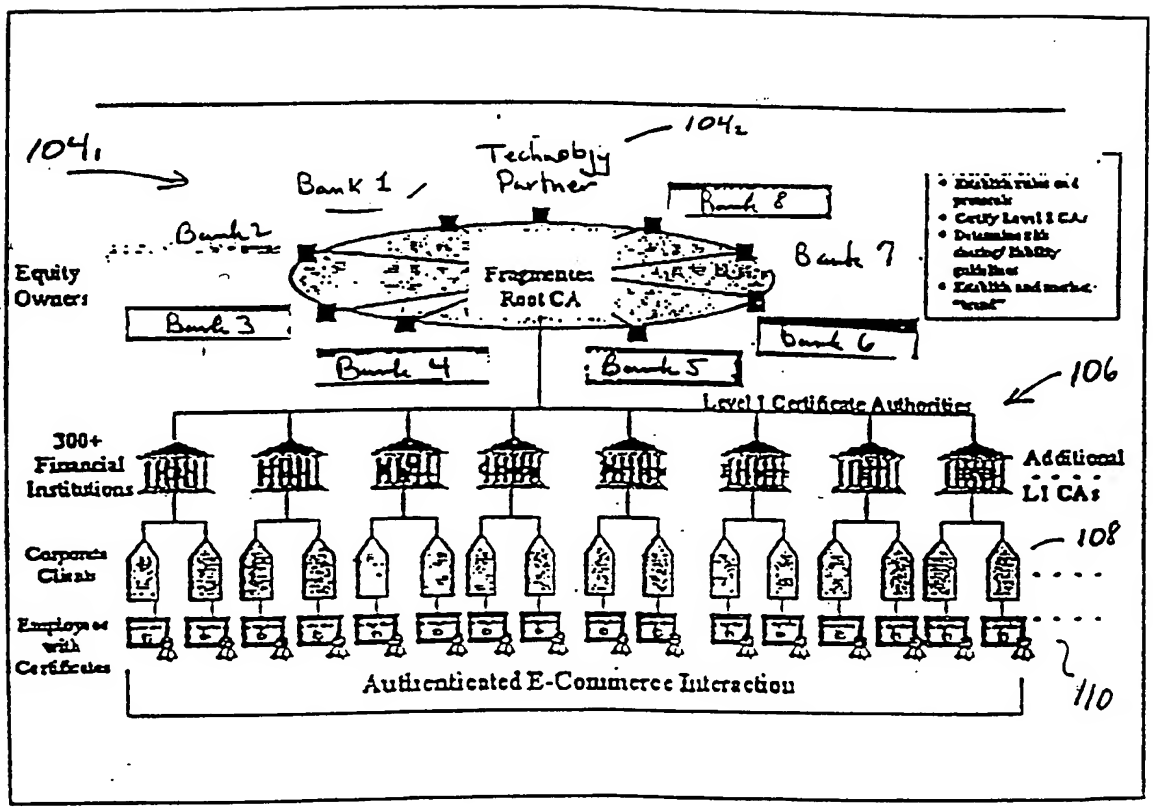

104₁
Technology Partner
104₂
Bank 1
Bank 2
Bank 3
Bank 4
Bank 5
Bank 6
Bank 7
Bank 8
Equity Owners
Fragmented Root CA
106
Level 1 Certificate Authorities
300+ Financial Institutions
Additional L1 CAs
Corporate Clients
108
Employees with Certificates
Authenticated E-Commerce Interaction
110

Fig. 1

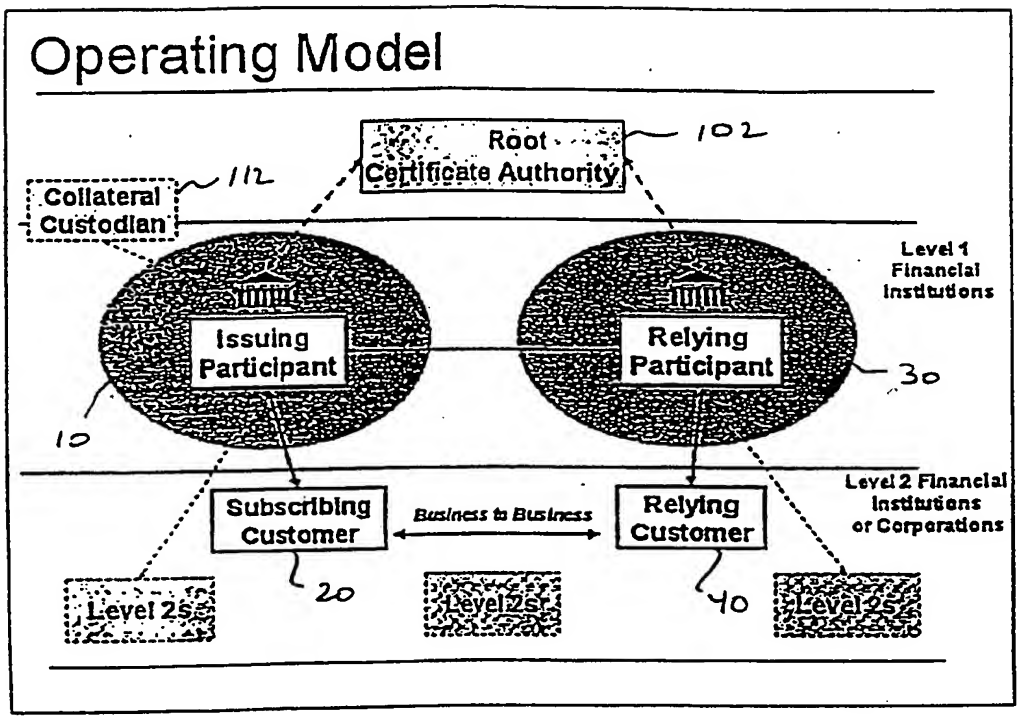

Operating Model
Root Certificate Authority
102
Collateral Custodian
112
Level 1 Financial Institutions
Issuing Participant
Relying Participant
30
10
Level 2 Financial Institutions or Corporations
Subscribing Customer
Business to Business
Relying Customer
20
40
Level 2s
Level 2s
Level 2s

Fig. 2

Figure 6

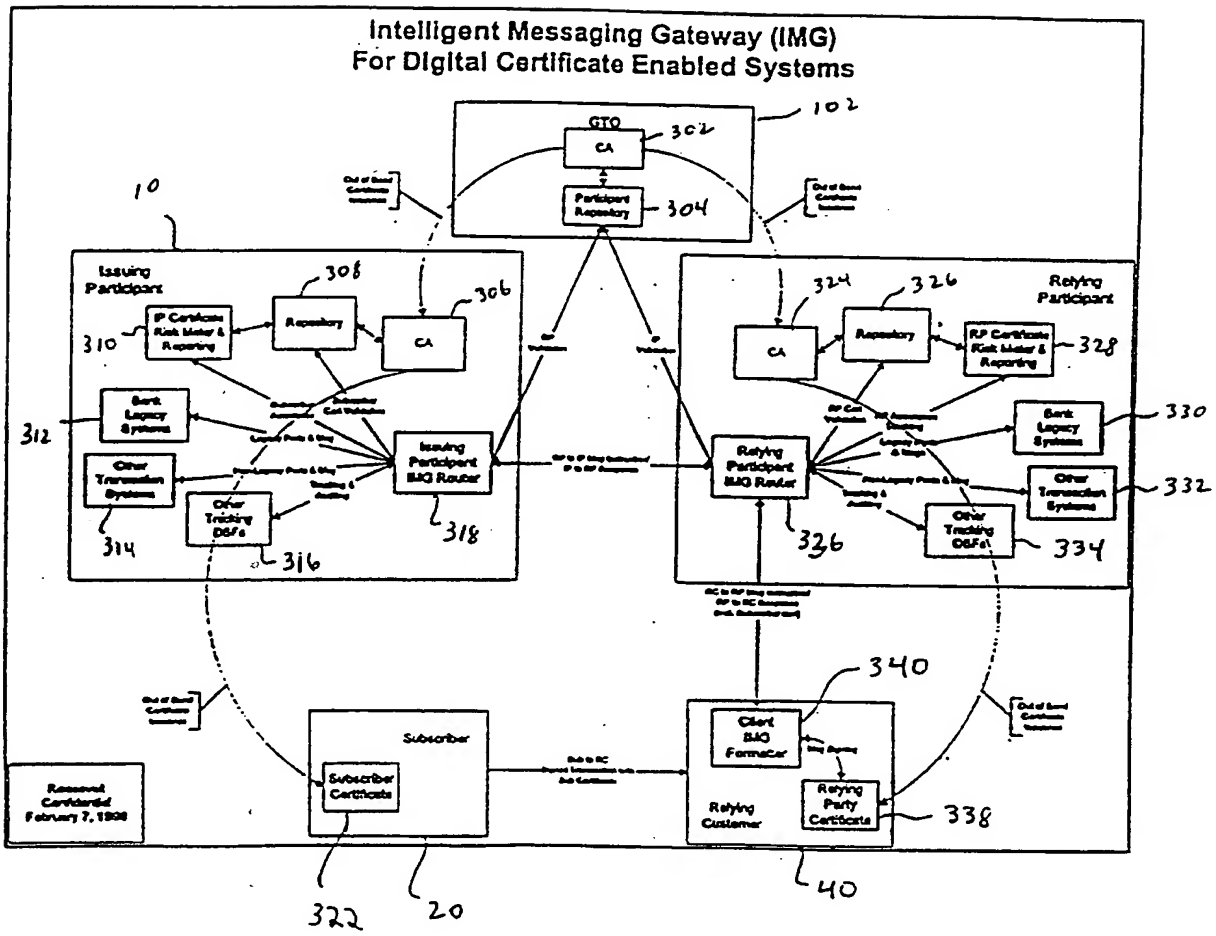
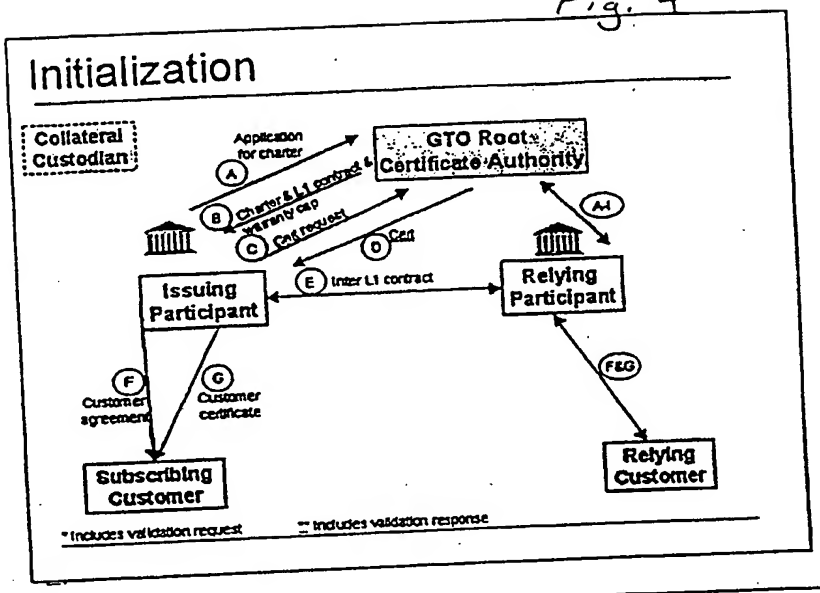


Fig. 3

Fig. 4


Initialization
Collateral Custodian
Application for charter
A
GTO Root Certificate Authority
B
Charter & L1 contract & warranty cap
C
Cert request
D
Cert
A1
Issuing Participant
E
Inter L1 contract
Relying Participant
F
Customer agreement
G
Customer certificate
F&G
Subscribing Customer
Relying Customer
* Includes validation request
= Includes validation response

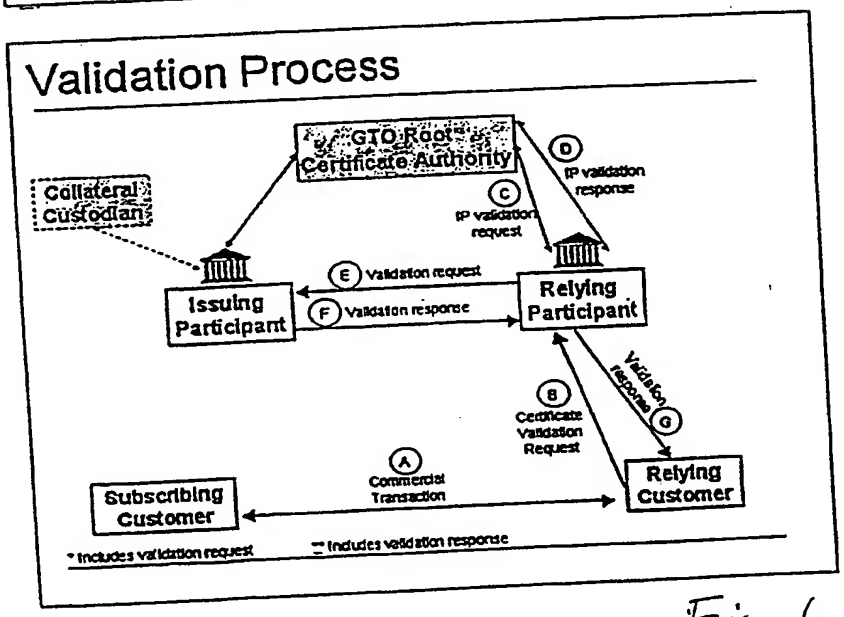

Validation Process
GTO Root Certificate Authority
D
IP validation response
C
IP validation request
Collateral Custodian
E
Validation request
F
Validation response
Issuing Participant
Relying Participant
B
Certificate Validation Request
Validation response
G
A
Commercial Transaction
Subscribing Customer
Relying Customer
* Includes validation request
= Includes validation response

Fig. 6

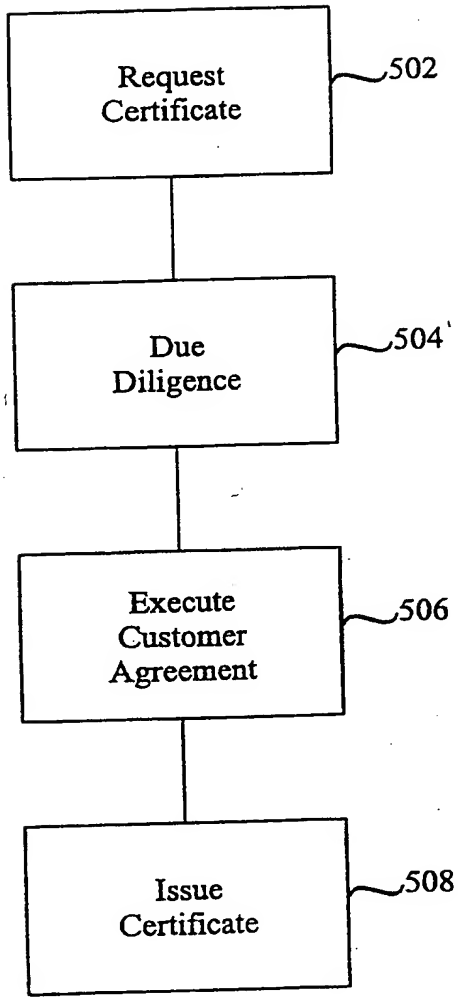

Request Certificate
502
Due Diligence
504
Execute Customer Agreement
506
Issue Certificate
508

Fig. 5

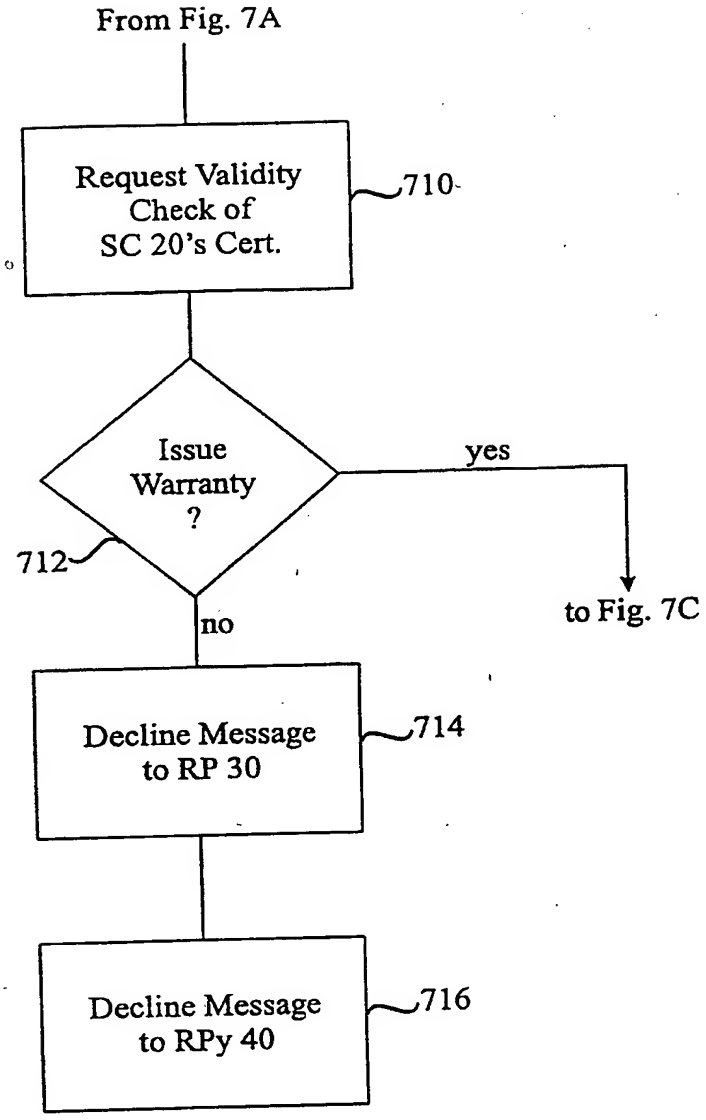

From Fig. 7A
Request Validity Check of SC 20's Cert.
710
Issue Warranty ?
712
yes
to Fig. 7C
no
Decline Message to RP 30
714
Decline Message to RPy 40
716

Fig. 7B

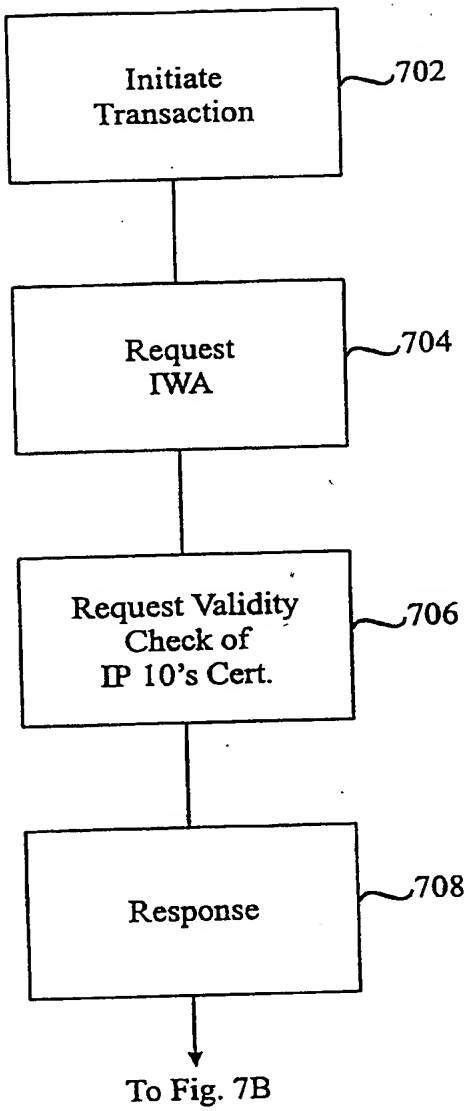

Initiate Transaction
702
Request IWA
704
Request Validity Check of IP 10's Cert.
706
Response
708
To Fig. 7B

Fig. 7A

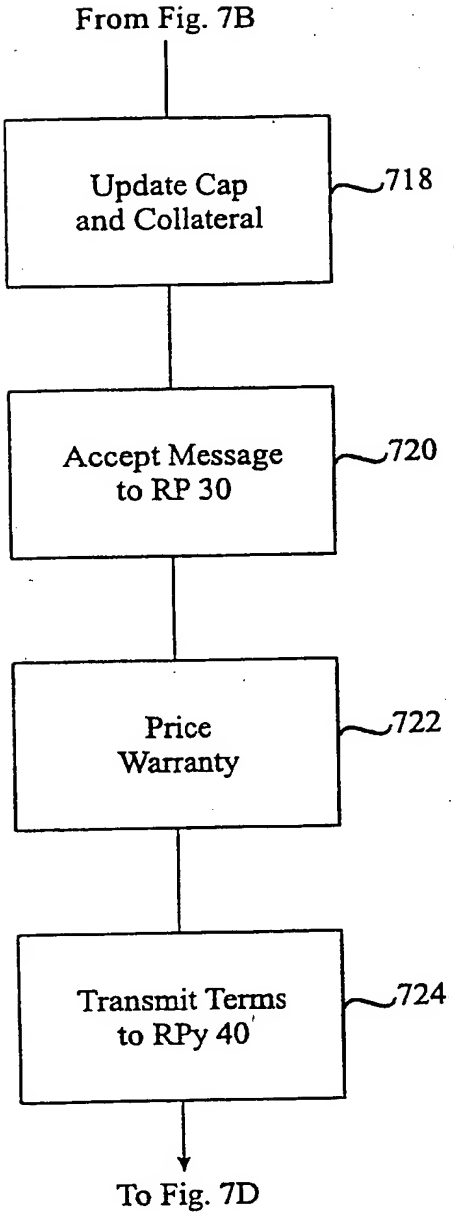

From Fig. 7B
Update Cap and Collateral
718
Accept Message to RP 30
720
Price Warranty
722
Transmit Terms to RPy 40
724
To Fig. 7D

Fig. 7C

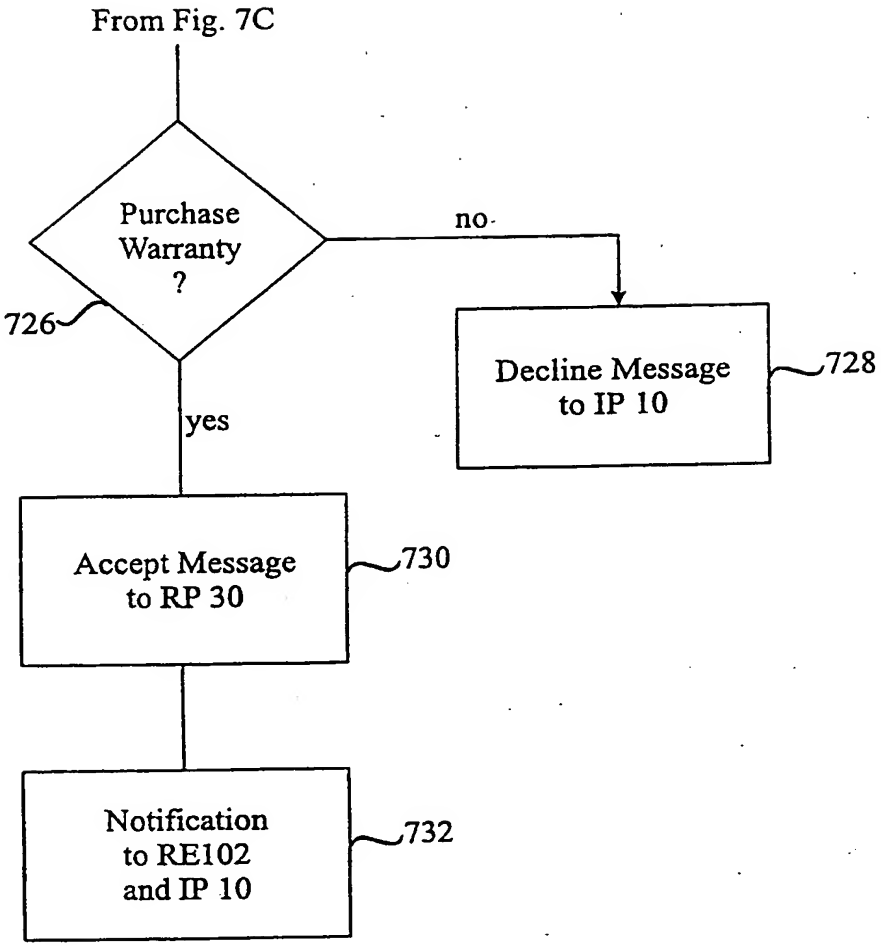
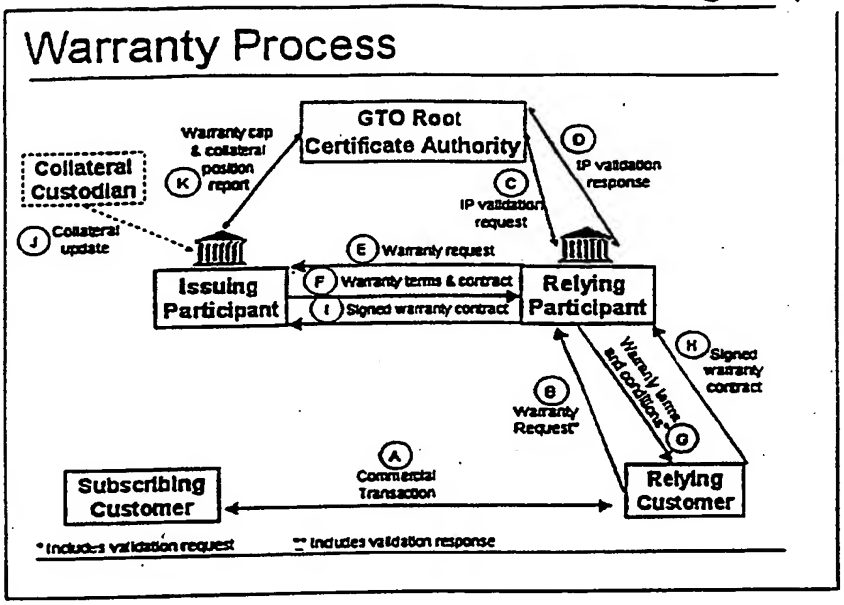

From Fig. 7C
Purchase Warranty ?
726
no
Decline Message to IP 10
728
yes
Accept Message to RP 30
730
Notification to RE102 and IP 10
732

Fig. 7D

Fig. 7E


Warranty Process
GTO Root Certificate Authority
Warranty cap & collateral position report
K
D
IP validation response
C
IP validation request
Collateral Custodian
J
Collateral update
E
Warranty request
Issuing Participant
F
Warranty terms & contract
I
Signed warranty contract
Relying Participant
H
Signed warranty contract
B
Warranty Request*
Warranty terms and conditions**
G
A
Commercial Transaction
Subscribing Customer
Relying Customer
* Includes validation request
** Includes validation response

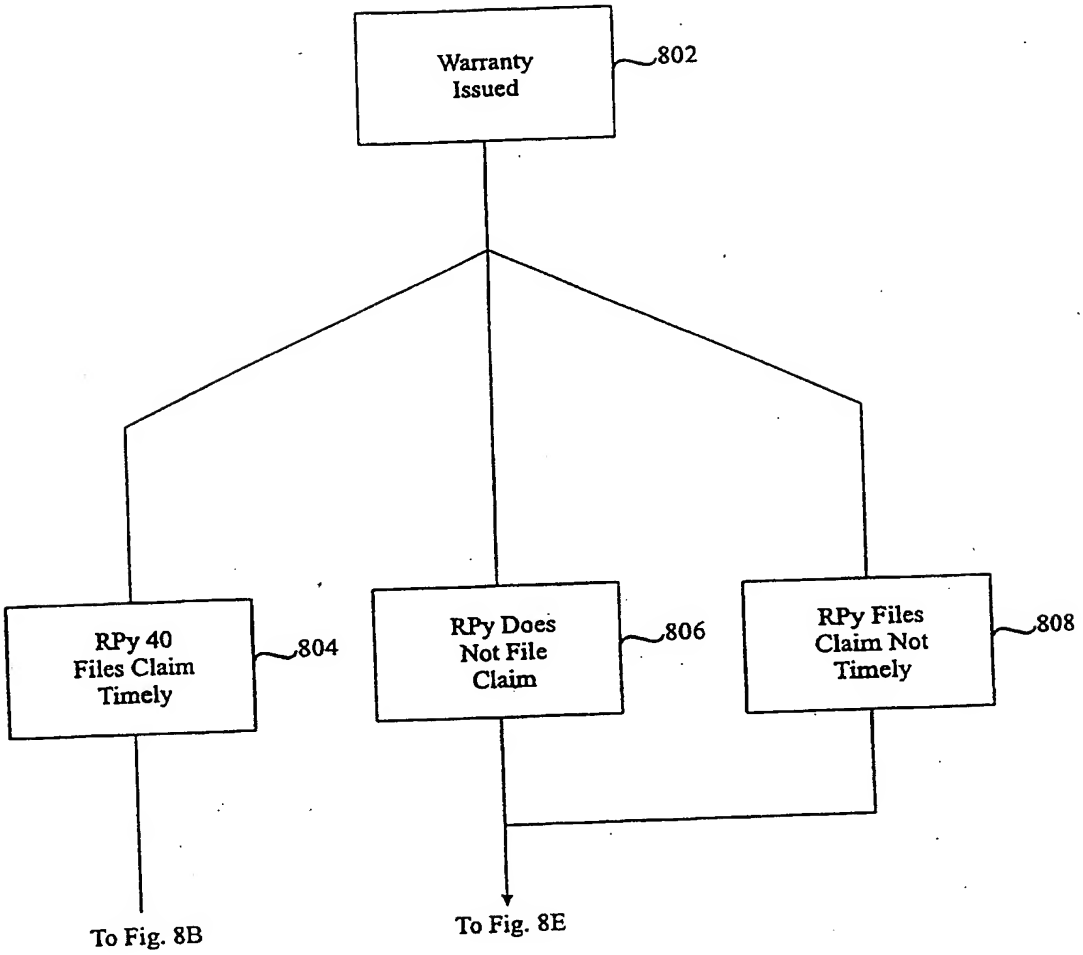

Warranty Issued
802
RPy 40 Files Claim Timely
804
RPy Does Not File Claim
806
RPy Files Claim Not Timely
808
To Fig. 8B
To Fig. 8E

Fig. 8A

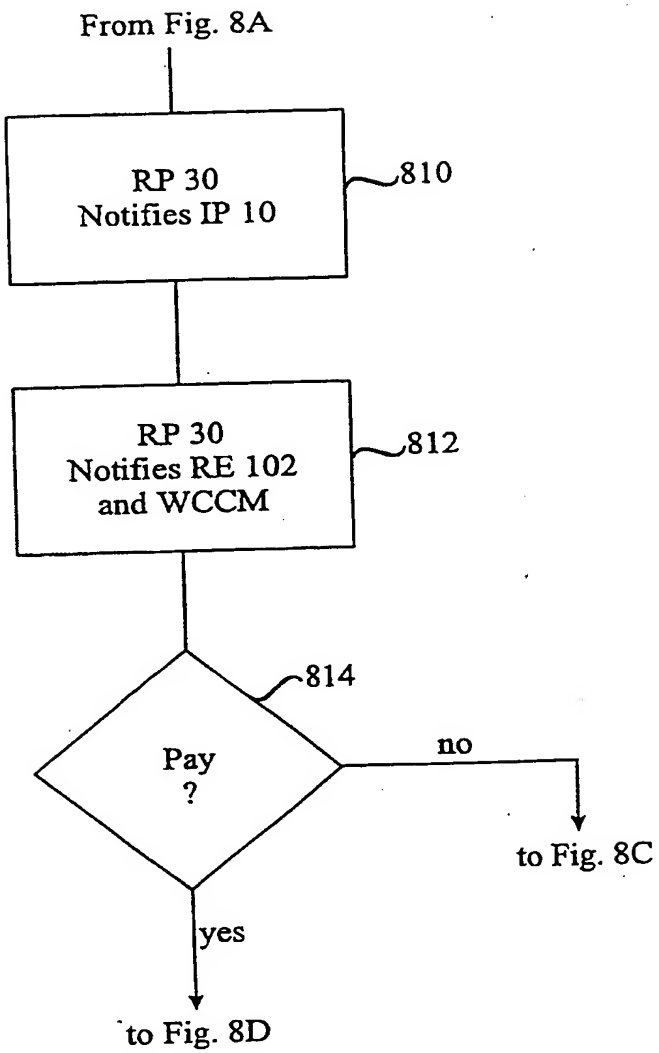

From Fig. 8A
RP 30
Notifies IP 10
810
RP 30
Notifies RE 102
and WCCM
812
814
Pay
?
no
to Fig. 8C
yes
to Fig. 8D

Fig. 8B

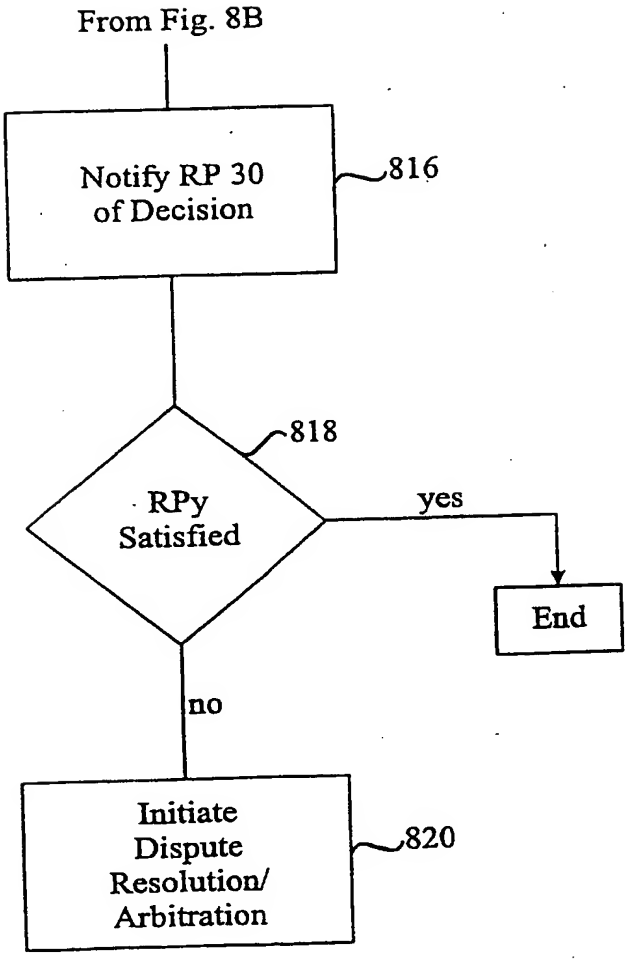

From Fig. 8B
Notify RP 30 of Decision
816
818
RPy Satisfied
yes
End
no
Initiate Dispute Resolution/ Arbitration
820

Fig. 8C

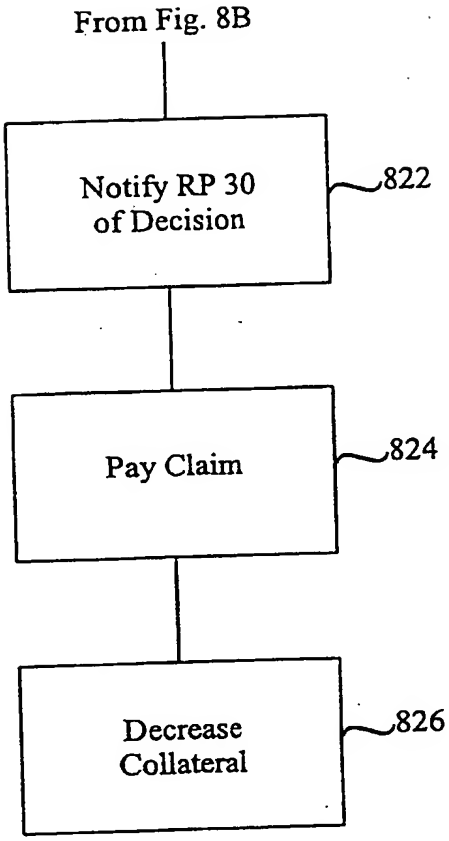

From Fig. 8B
Notify RP 30 of Decision
822
Pay Claim
824
Decrease Collateral
826

Fig. 8D

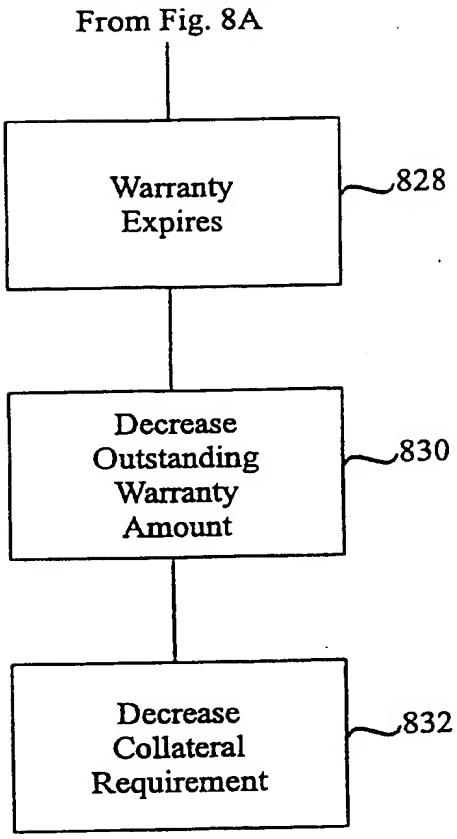

From Fig. 8A
Warranty Expires
828
Decrease Outstanding Warranty Amount
830
Decrease Collateral Requirement
832

Fig. 8E

Fig. 8F

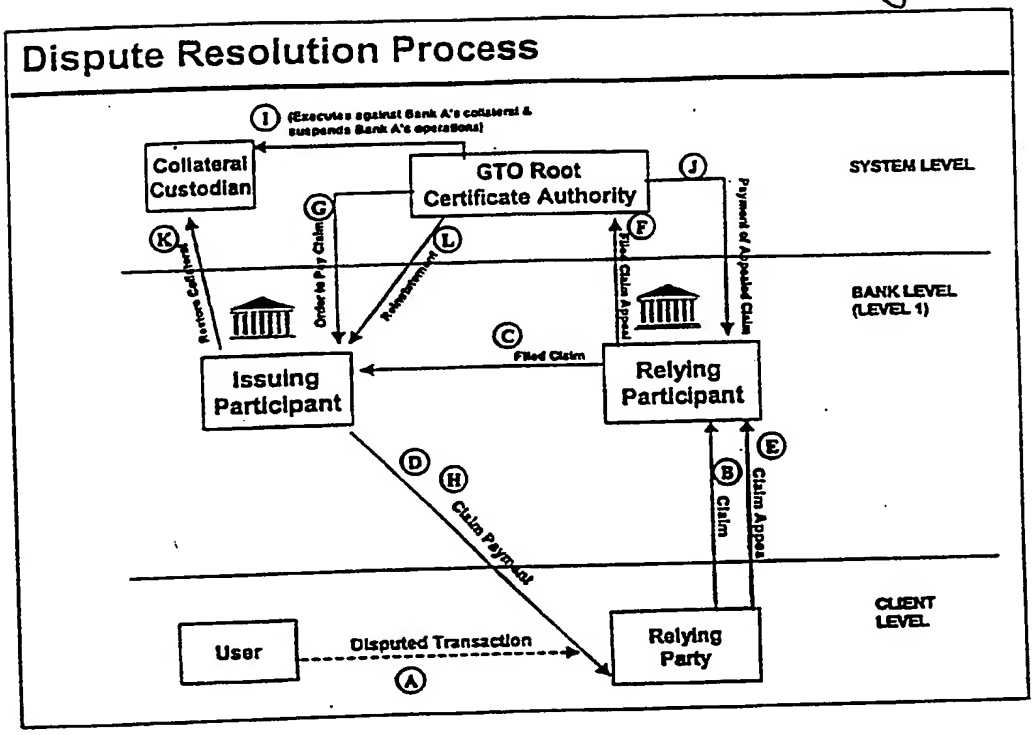
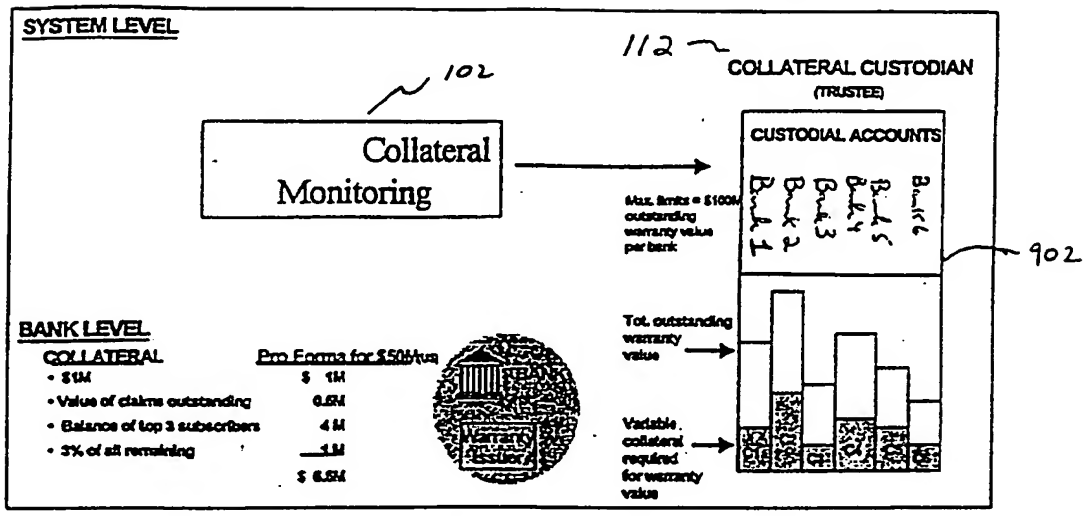

Dispute Resolution Process
(1) (Executes against Bank A's collateral & suspends Bank A's operations)
Collateral Custodian
GTO Root Certificate Authority
SYSTEM LEVEL
BANK LEVEL (LEVEL 1)
Issuing Participant
Relying Participant
Filed Claim
Claim Payment
Claim
Claim Appeal
Disputed Transaction
User
Relying Party
CLIENT LEVEL

Fig. 9


SYSTEM LEVEL
102
Collateral Monitoring
112
COLLATERAL CUSTODIAN
(TRUSTEE)
CUSTODIAL ACCOUNTS
Bank 1
Bank 2
Bank 3
Bank 4
Bank 5
Bank 6
902
Max. limits = $100M outstanding warranty value per bank
Tot. outstanding warranty value
Variable collateral required for warranty value
BANK LEVEL
COLLATERAL
Pro Forma for $50M/us
• $1M
$ 1M
• Value of claims outstanding
0.5M
• Balance of top 3 subscribers
4 M
• 3% of all remaining
1 M
$ 6.5M
Warranty Issuer

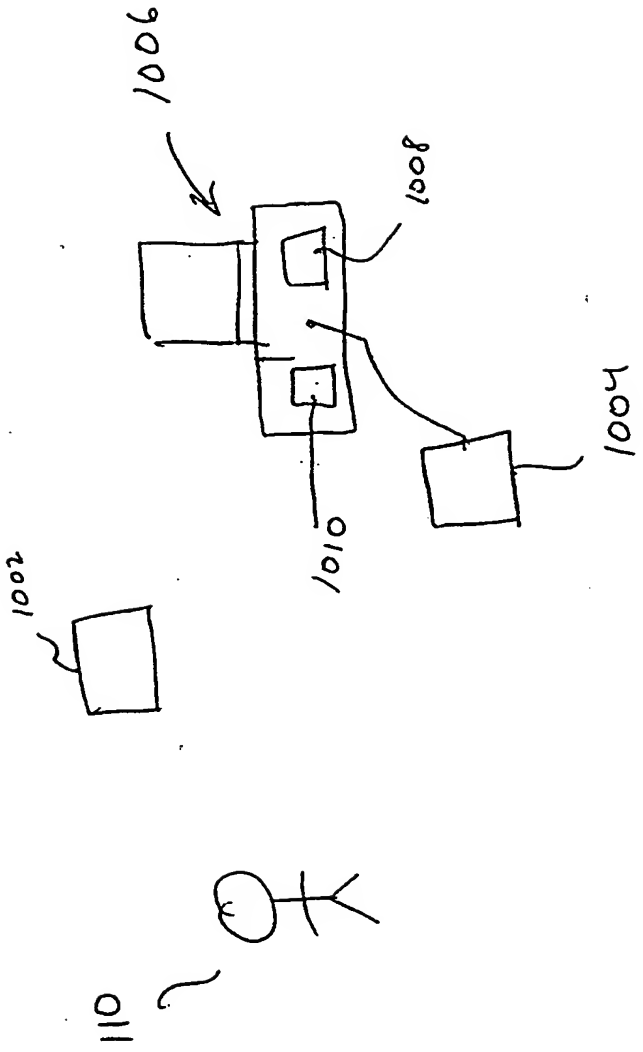


Fig. 10

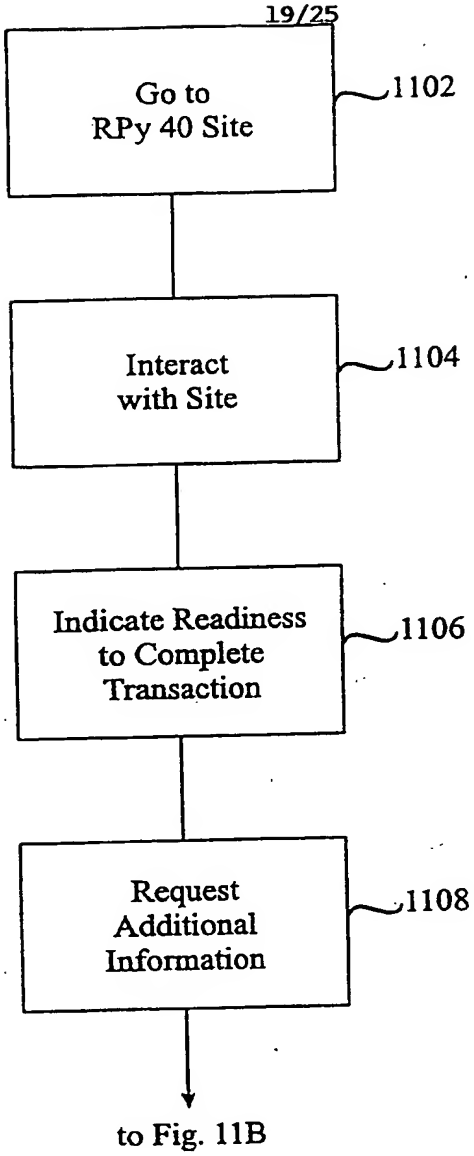

Go to
RPy 40 Site
1102
Interact
with Site
1104
Indicate Readiness
to Complete
Transaction
1106
Request
Additional
Information
1108
to Fig. 11B

Fig. 11A

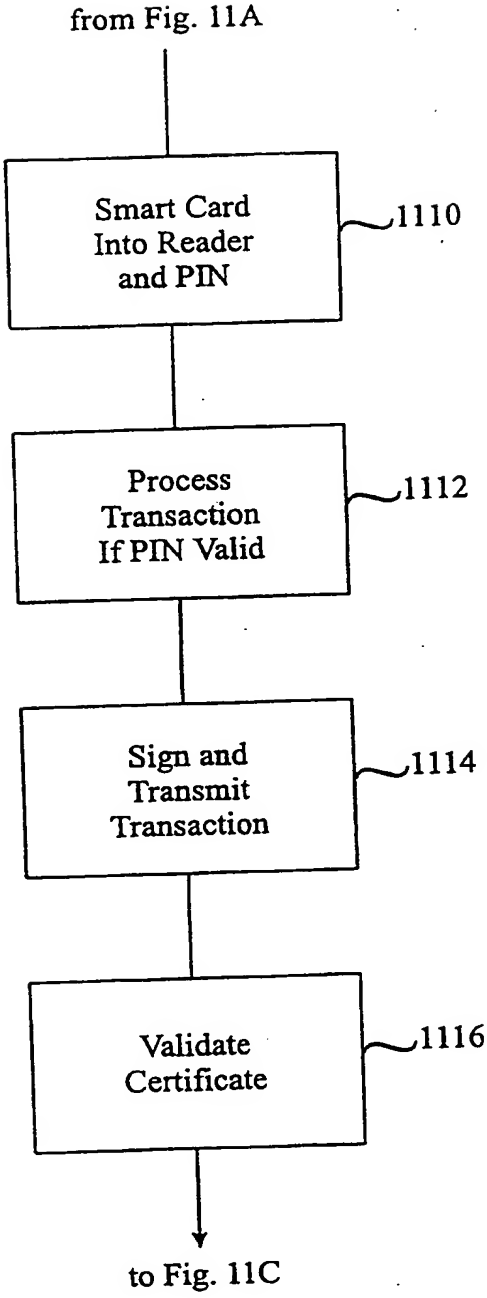

from Fig. 11A
Smart Card Into Reader and PIN
1110
Process Transaction If PIN Valid
1112
Sign and Transmit Transaction
1114
Validate Certificate
1116
to Fig. 11C

Fig. 11B

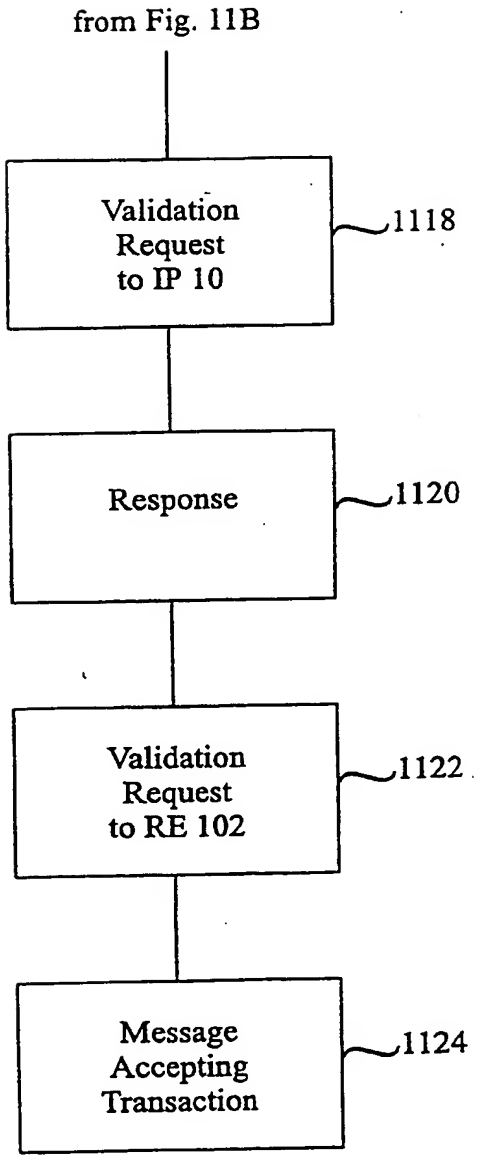

from Fig. 11B
Validation Request to IP 10
1118
Response
1120
Validation Request to RE 102
1122
Message Accepting Transaction
1124

Fig. 11C

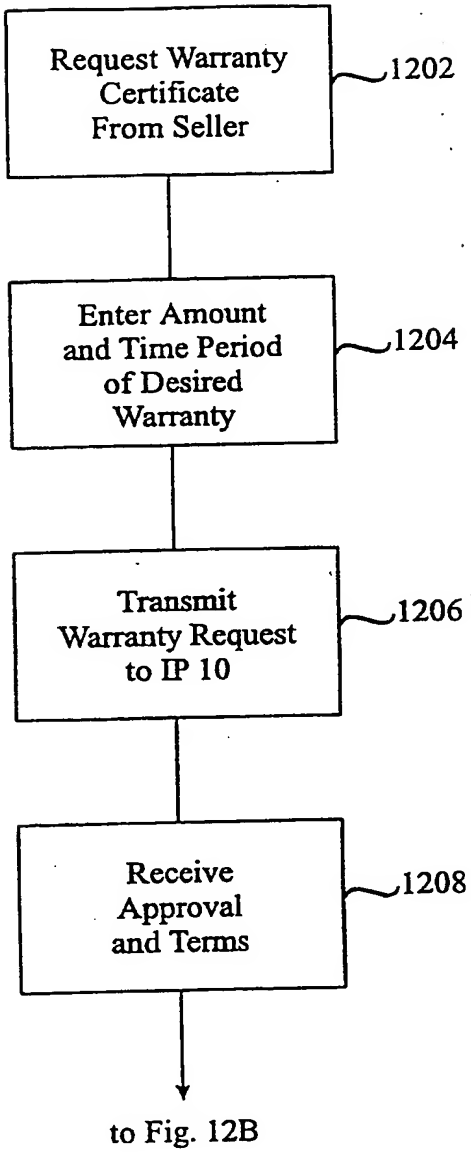

Request Warranty Certificate From Seller
1202
Enter Amount and Time Period of Desired Warranty
1204
Transmit Warranty Request to IP 10
1206
Receive Approval and Terms
1208
to Fig. 12B

Fig. 12A

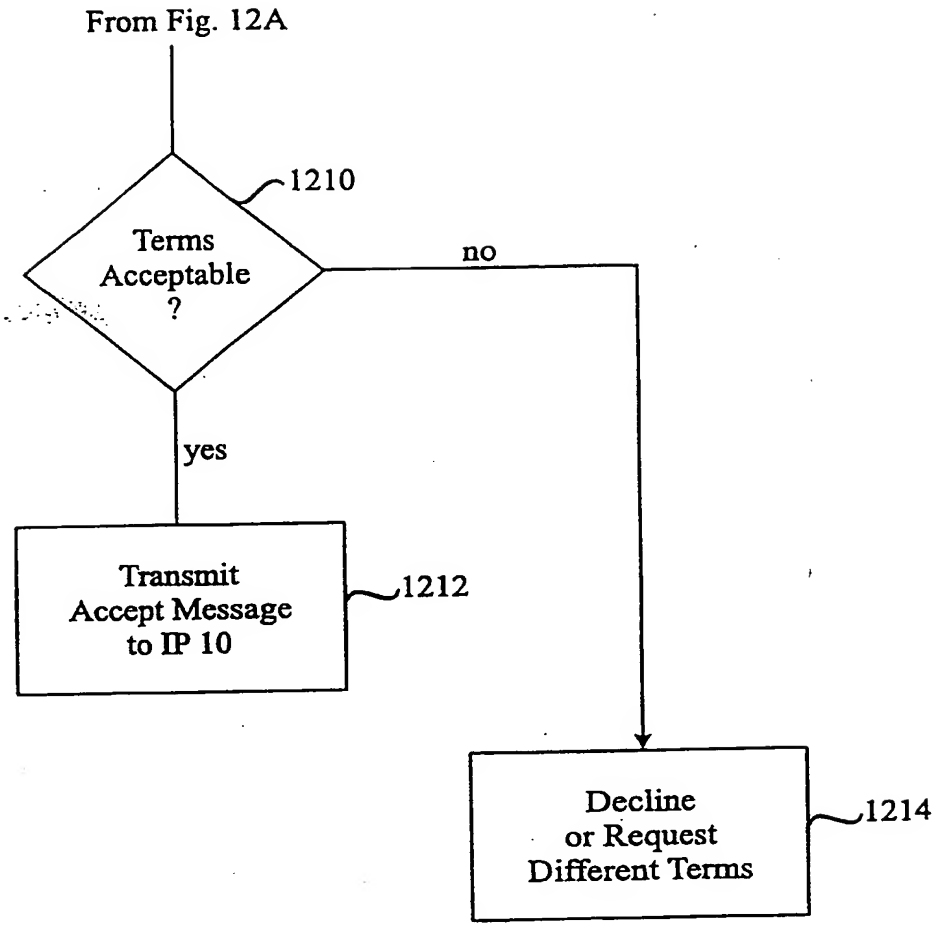

From Fig. 12A
1210
Terms Acceptable ?
no
yes
Transmit Accept Message to IP 10
1212
Decline or Request Different Terms
1214

Fig. 12B

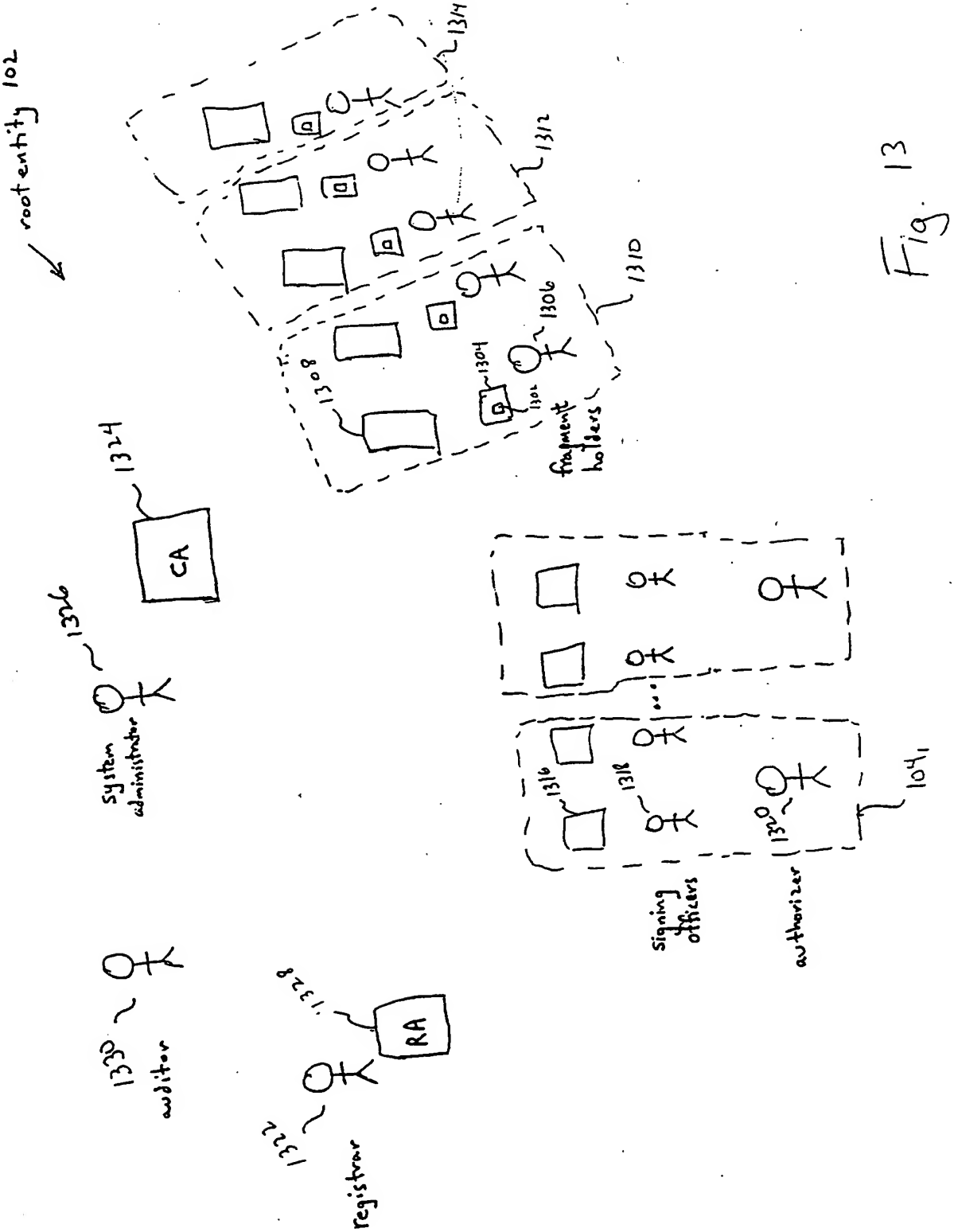

root entity 102
1314
1312
1310
1306
1304
1302
1308
fragment holders
1324
CA
1326
system administrator
1330
auditor
1328
RA
1322
registrar
1316
1318
1320
1041
signing officers
authorizer

Fig. 13

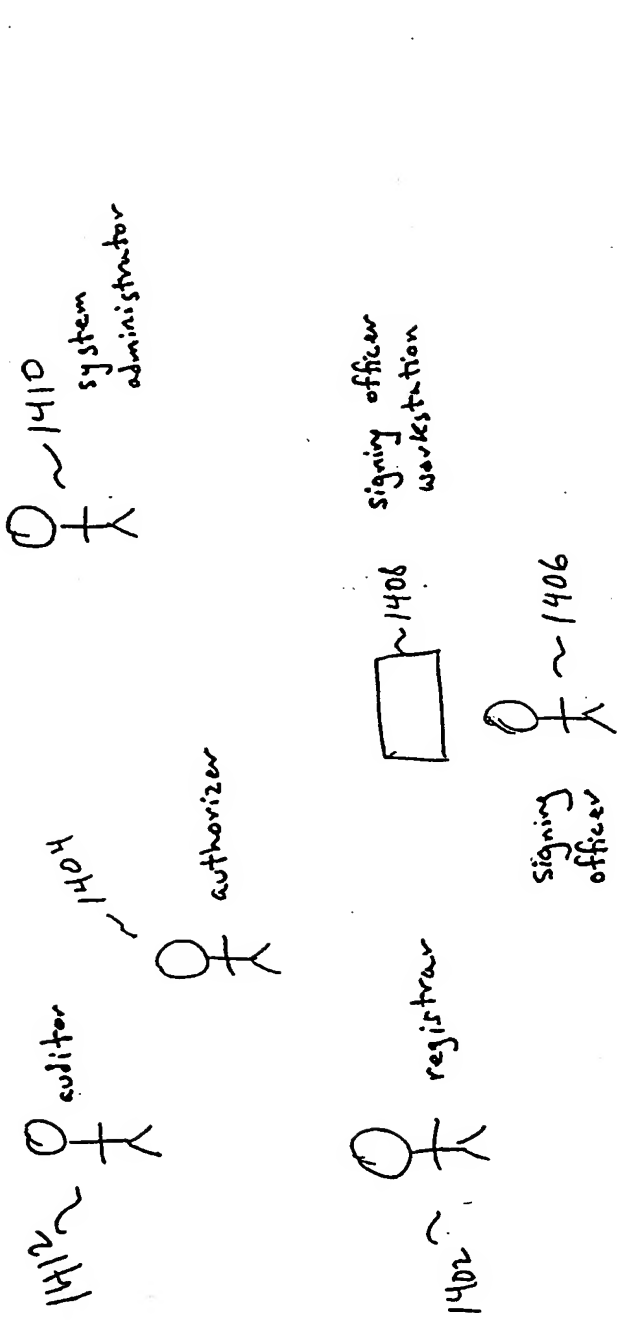

1410
system administrator
1408
signing officer workstation
1406
signing officer
1404
authorizer
1402
registrar
1412
auditor
L1 participants 106

Fig. 14

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/03550

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/32
US CL : 705/44,75,76; 713/150,156,157
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 705/44,75,76; 713/150,156,157

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WEST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,659,616 A (SUDIA) 19 August 1997 (19.08.1997) column 3, lines 48-67; column 4, lines 29-38; column 7, line 35 to column 9, line 10; column 14, line 20 to column 16, line 29.	1,14,16-19 and 26-28
X,P	US 5,903,882 A (ASAY et al) 11 May 1999 (11.05.1999), column 4, line 20 to column 9, line 10; column 21, line 47 to column 23, line 67; column 24, line 17 to column 25, line 7.	1-28

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
	02 MAY 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Tod R Swann James R. Matthews Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)